

MANUAL

DOE M 470.4-4A

Approved: 1-16-09

INFORMATION SECURITY MANUAL



U.S. Department of Energy
Office of Health, Safety and Security

AVAILABLE ONLINE AT:
www.directives.doe.gov

INITIATED BY:
Office of Health, Safety and Security

INFORMATION SECURITY

1. PURPOSE. This Manual establishes security requirements for the protection and control of matter required to be classified or controlled by statutes, regulations, or U.S. Department of Energy (DOE) directives. All information security programs, practices, and procedures developed within DOE must be consistent with and incorporate the requirements of this Manual along with all of the national requirements (Atomic Energy Act, Executive Orders, *Code of Federal Regulations*, United States Code, National Industrial Security Operations Manual, etc.). All these national information security requirements must be reviewed and incorporated because requirements have not been repeated in this Manual. DOE M 470.4-7, *Safeguards and Security Program References*, Section B, under Information Security, contains a list of national policies. DOE M 470.4-7 also contains definitions, acronyms, and references that apply to the Safeguards and Security Program. Paragraph 9 below also provides references. Whenever requirements from multiple source documents pertain, the most restrictive requirement(s) apply. Deviations from national requirements are subject to the deviation process of the governing document rather than the DOE deviation process. The information security program includes Classified Matter Protection and Control (CMPC), security of classified Foreign Government Information, Operations Security (OPSEC), security of Special Access Programs (SAP), and Technical Surveillance Countermeasures (TSCM).
2. CANCELLATIONS. DOE M 470.4-4, Change 1, *Information Security*, dated 06-29-07, except for Section E – Technical Surveillance Countermeasures, which will be retained in its entirety as Section D of this Manual. Cancellation of a directive does not, by itself, modify or otherwise affect any contractual obligation to comply with the Manual. Canceled Manuals that are incorporated by reference in a contract remain in effect until the contract is modified to delete the reference to the requirements in the canceled Manuals.
3. APPLICABILITY.
 - a. All Departmental Elements. Except for the exclusion in paragraph 3.c, this Manual applies to all Departmental elements (see <http://www.directives.doe.gov/pdfs/reftools/org-list.pdf> for a complete list of all Departmental elements). This Manual automatically applies to Departmental elements created after it is issued.

The Administrator of the National Nuclear Security Administration (NNSA) will ensure that NNSA employees and contractors comply with their respective responsibilities under this Manual.
 - b. DOE Contractors.
 - (1) Except for the exclusions in paragraph 3.c, the Contractor Requirements Document (CRD), Attachment 1, sets forth requirements of this Manual that will apply to site/facility management contracts that include the CRD.

- (2) The CRD must be included in the site/facility management contracts that involve classified matter or nuclear materials and contain DOE Acquisition Regulation (DEAR) clause 952.204-2, titled *Security Requirements*.
 - (a) Departmental elements must notify contracting officers of affected site/facility management contracts to incorporate this Manual into those contracts.
 - (b) Once notified, contracting officers are responsible for incorporating this directive into the affected contracts via the Laws, regulations, and DOE directives clause of the contracts.
- (3) A violation of the provisions of the CRD relating to the safeguarding or security of Restricted Data or other classified information may result in a civil penalty pursuant to subsection a. of section 234B of the Atomic Energy Act of 1954 (42 U.S.C. 2282b). The procedures for the assessment of civil penalties are set forth in Title 10, *Code of Federal Regulations* (CFR), Part 824, "Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations."
- (4) As stated in DEAR clause 970.5204-2, titled *Laws, Regulations, and DOE Directives*, regardless of the performer of the work, site/facility contractors that have the CRD incorporated into their contracts are responsible for compliance with the CRD. Affected site/facility management contractors are responsible for flowing down the requirements of the CRD to subcontracts at any tier to the extent necessary to ensure compliance with the requirements. In doing so, contractors must not unnecessarily or imprudently flow down requirements to subcontracts. That is, contractors must both ensure that they and their subcontractors comply with the requirements of this CRD and only incur costs that would be incurred by a prudent person in the conduct of competitive business.
- (5) This Manual does not automatically apply to other than site/facility management contracts. Application of any of the requirements of this Manual to other than site/facility management contracts will be communicated as follows:
 - (a) Heads of Field Elements and Headquarters Departmental Elements. Review procurement requests for new non-site/facility management contracts that involve classified matter or nuclear materials and contain DEAR clause 952.204-2, *Security Requirements*, and ensure that the requirements of the CRD of this Manual are included in those contracts.
 - (b) Contracting Officers. Assist originators of procurement requests who want to incorporate the requirements of the CRD of this

Manual in new non-site/facility management contracts, as appropriate.

- c. Exclusion. In accordance with the responsibilities and authorities assigned by Executive Order 12344 and to ensure consistency throughout the joint Navy and DOE organization of the Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors will implement and oversee all requirements and practices pertaining to this Manual for activities under the Deputy Administrator's cognizance.
4. REQUIREMENTS. Detailed requirements are included in each Chapter of this Manual.
5. RESPONSIBILITIES. See DOE O 470.4A, *Safeguards and Security Program*, dated 05-25-07, for specific responsibilities.
6. SUMMARY. This Manual consists of four sections that provide direction for CMPC, OPSEC, security of SAP, and TSCM. Section A, CMPC, has three chapters. Chapter I provides the CMPC planning. Chapter II provides the CMPC requirements. Chapter III provides storage requirements for classified matter. Section B provides requirements for OPSEC. Section C presents requirements for SAP. Section D provides requirements for TSCM. Attachment 1 contains the CRD for extending the requirements of this Manual to DOE contractors and subcontractors.
7. DEVIATIONS. Deviations from national regulations, including the CFR and national-level policies are subject to the deviation process of the governing document rather than the DOE deviation process. This directive conveys no authority to deviate from law. Requests for deviations from requirements specific to DOE, including this Manual, must be processed in accordance with the provisions of DOE M 470.4-1 Chg. 1, *Safeguards and Security Program Planning and Management*.
8. DEFINITIONS. Terms used in the DOE Safeguards and Security program are defined in the S&S Glossary in DOE M 470.4-7, *Safeguards and Security Program References*.
9. REFERENCES.
 - a. References commonly used in the Safeguards and Security Program are located in DOE M 470.4-7.
 - b. Title XXXII of P.L. 106-65, National Nuclear Security Administration Act, as amended, which established a separately organized agency within DOE.
 - c. The following references include additional information security requirements:
 - (1) 18 U.S.C. 798, Disclosure of Classified Information.
 - (2) 42 U.S.C., Chapter 23. [Atomic Energy Act of 1954 (AEA), as amended].
 - (3) 50 U.S.C. 2426, Congressional Oversight of Special Access Programs.

- (4) Title 10, Code of Federal Regulations, Energy, Parts 725, 824, 1016, 1017, 1044, 1045, and 1046.
- (5) Title 32 Code of Federal Regulations, Chapter XIX, Central Intelligence Agency.
- (6) Title 32 Code of Federal Regulations, Chapter XX, Information Security Oversight Office, *National Archives and Records Administration*.
- (7) Title 48 Code of Federal Regulations, Chapter 9, Department of Energy (DEAR 952.204).
- (8) Executive Order 12333, United States Intelligence Activities.
 - (a) Amended by: EO 13284, Amendment of Executive Orders, and Other Actions, in Connection With the Establishment of the Department of Homeland Security.
 - (b) Amended by: EO 13355, Strengthened Management of the Intelligence Community.
- (9) Executive Order 12829, National Industrial Security Program.
 - (a) Amended by E.O. 12885, Amendment to Executive Order No. 12829.
- (10) Executive Order 12958, Classified National Security Information.
 - (a) Amended by E.O. 12972, Amendment to Executive Order No. 12958.
 - (b) Amended by E.O. 13142, Amendment to Executive Order 12958, Classified National Security Information.
 - (c) Amended by E.O. 13292, Further Amendment to Executive Order 12958, as Amended, Classified National Security Information.
- (11) Executive Order 12968, Access to Classified Information.
- (12) Executive Order 13462, President's Intelligence Advisory Board and Intelligence Oversight Board.
- (13) National Security Decision Directive 19, Protection of Classified National Security Council and Intelligence Information.
- (14) National Security Decision Directive 84, Safeguarding National Security Information.

- (15) National Security Decision Directive 298, National Operations Security Program.
- (16) NDP-1, National Policies and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organization.
- (17) National Industrial Security Program Operating Manual.
- (18) National Industrial Security Program Operating Manual Operating Manual Supplement.
- (19) NAVSEAINST C5511.32B, Safeguarding of Naval Nuclear Propulsion Information (NNPI) (U).
- (20) Security Policy Board Issuance 4-97, National Policy on Reciprocity of Use and Inspection of Facilities.
- (21) Security Policy Board SPB Issuance 5-97, Guidelines for the Implementation and Oversight of the Policy on Reciprocity of Use and Inspection of Facilities.
- (22) DOE O 200.1, *Information Management Program*, dated 9-30-96.
- (23) DOE M 200.1-1 Chapter 9, *Public Key Cryptography and Key Management*, dated 2-15-00.
- (24) DOE P 205.1, *Departmental Cyber Security Management Policy*, dated 5-8-01.
- (25) DOE M 205.1-3, *Telecommunications Security Manual*, dated 4-17-06.
- (26) DOE M 205.1-4, *National Security System Manual*, dated 3-8-07.
- (27) DOE M 205.1-5, *Cyber Security Process Requirements Manual*, dated 8-12-08.
- (28) DOE O 205.1A, *Department of Energy Cyber Security Management*, 12-4-06.
- (29) DOE O 241.1A Chg 1, *Scientific and Technical Information Management*, dated 10-14-03.
- (30) DOE M 452.4-1A, *Protection of Use Control Vulnerabilities and Designs*, dated 3-11-04.
- (31) DOE P 470.1, *Integrated Safeguards and Security Management (ISSM) Policy*, dated 5-8-01.

- (32) DOE O 470.3B, *Graded Security Protection (GSP) Policy*, dated 8-12-08.
- (33) DOE M 470.4-1 Chg 1, *Safeguards and Security Program Planning and Management*, dated 8-26-05.
- (34) DOE G 470.4-1, *Asset Protection Analysis Guide*, dated 8-21-08.
- (35) DOE M 470.4-2 Chg 1, *Physical Protection*, dated 8-26-05.
- (36) DOE M 470.4-3 Chg 1, *Protective Force*, dated 8-26-05.
- (37) DOE M 470.4-5, *Personnel Security*, dated 8-26-05.
- (38) DOE M 470.4-6 Chg 1, *Nuclear Material Control and Accountability*, dated 8-26-05.
- (39) DOE M 470.4-7, *Safeguards and Security Program References*, dated 8-26-05.
- (40) DOE O 470.4A, *Safeguards and Security Program*, dated 5-25-07.
- (41) DOE M 471.1-1 Chg 1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual*, dated 10-23-01.
- (42) DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*, dated 6-30-00.
- (43) DOE M 471.2-3B, *Special Access Program Policies, Responsibilities, and Procedures*, dated 10-29-07.
- (44) DOE O 471.3, *Identifying and Protecting Official Use Only Information*, dated 4-9-03.
- (45) DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, dated 4-9-03.
- (46) DOE G 471.3-1, *Guide to Identifying Official Use Only Information*, dated 4-9-03.
- (47) DOE O 475.1, *Counterintelligence Program*, dated 12-10-04.
- (48) DOE M 475.1-1 B, *Manual for Identifying Classified Information*, dated 8-28-07.
- (49) DOE O 475.2, *Identifying Classified Information*, dated 8-28-07.
- (50) DOE O 5610.2 Chg 1, *Control of Weapon Data*, dated 9-2-86.

- (51) DOE O 5639.8A, *Security of Foreign Intelligence Information and Sensitive*, dated 7-23-93.
 - (52) Compartmented Information Facilities.
 - (53) DOE O 5670.1A, *Management and Control of Foreign Intelligence*, dated 1-15-92.
 - (54) DOE Sensitive Compartmented Information Facility Procedural Guide.
10. IMPLEMENTATION. Requirements that cannot be implemented within 6 months of the effective date of this Manual or with existing resources must be documented by the cognizant security authority and submitted to the relevant program officers; the Under Secretary for Energy, the Under Secretary for Science, or the Under Secretary for Nuclear Security/Administrator, NNSA; and the Office of Health, Safety and Security. The documentation must include timelines and resources needed to fully implement this Manual. The documentation must also include a description of the vulnerabilities and impacts created by the delayed implementation of the requirements.
11. CONTACT. Questions concerning this Manual should be directed to the Office of Security Policy, Office of Health, Safety and Security at (301) 903-4053.

BY ORDER OF THE SECRETARY OF ENERGY:



JEFFREY F. KUPFER
Acting Deputy Secretary

TABLE OF CONTENTS

INFORMATION SECURITY	I
1. Purpose.....	i
2. Cancellations.....	i
3. Applicability	i
4. Requirements	iii
5. Responsibilities.....	iii
6. Summary	iii
7. Deviations	iii
8. Definitions.....	iii
9. References.....	iii
10. Implementation	ix
11. Contact	ix
 SECTION A —CLASSIFIED MATTER PROTECTION AND CONTROL	 A-1
1. Objectives	A-1
2. Requirements	A-1
 CHAPTER I . PROTECTION AND CONTROL PLANNING	 I-1
1. Classified Matter Protection and Control (CMPC) Program Implementation.....	I-1
2. Protection Strategies & Planning.....	I-1
3. Disclosure and Release of Classified Matter	I-1
4. Training.....	I-6
 CHAPTER II . CLASSIFIED MATTER PROTECTION AND CONTROL REQUIREMENTS	 II-1
1. General.....	II-1
2. Classified Matter in Use.....	II-2
3. Marking.....	II-3
4. Marking Material	II-8
5. Control Systems and Accountability	II-9

6.	Reproduction.....	II-14
7.	Receiving and Transmitting Classified Matter	II-15
8.	Destruction.....	II-24
9.	Foreign Government Information	II-26

CHAPTER III . STORAGE REQUIREMENTS FOR CLASSIFIED MATTER.....III-1

1.	Storage Requirements	III-1
2.	Storage—Repositories	III-3
3.	Non-Conforming Storage.....	III-6
4.	Permanent Burial	III-7

SECTION B —OPERATIONS SECURITY.....B-1

1.	Objectives	B-1
2.	Requirements	B-1

SECTION C —SPECIAL ACCESS PROGRAMS..... C-1

1.	Objectives	C-1
2.	Requirements	C-1

SECTION D —TECHNICAL SURVEILLANCE COUNTERMEASURES D-1

ATTACHMENT 1 — CONTRACTOR REQUIREMENTS DOCUMENT

SECTION A—CLASSIFIED MATTER PROTECTION AND CONTROL

1. OBJECTIVES.

- a. To protect and control classified matter that is generated, received, transmitted, used, stored, reproduced, permanently buried according to the requirements of this Manual, or to be destroyed.
- b. To establish the requirements for an audit trail for all accountable classified matter.
- c. To establish required controls based on classification level (Top Secret, Secret, or Confidential) and category (Restricted Data [RD], Formerly Restricted Data [FRD]), or National Security Information [NSI]) or special handling instructions or caveats.

2. REQUIREMENTS.

- a. Classified matter that is generated, received, transmitted, used, stored, reproduced, permanently placed (buried according to the requirements of this Manual), or destroyed must be protected and controlled commensurate with classification level, category (if RD/FRD), and caveats (if applicable). All pertinent attributes must be used to determine the degree of protection and control required to prevent unauthorized access to classified matter.
- b. Classified information must only be processed on information systems that have received authority to operate according to DOE Office of the Chief Information Officer directives that establish requirements for national security systems.
- c. Audit trails must be implemented for all accountable classified matter.
- d. Buildings and rooms containing classified matter must be configured with security measures, which prevent unauthorized persons from gaining access to classified matter; specifically, security measures that prevent unauthorized physical, visual, and aural access.
- e. Secret matter that cannot be processed, handled, and/or stored within a Limited Area (LA) or higher must be maintained in an accountability system as described in Chapter II of this Manual.
- f. Need-to-know controls, appropriate physical security, and access control measures must be applied to each area or building within a security area where classified matter is processed, handled or stored to detect unauthorized access.
- g. Retention Requirements. All records associated with the protection and control of classified matter must be maintained in accordance with the most current National Archives Records Administration General Records Schedule 18, *Security and Protective Services Record*.

- h. Reporting Requirements. Report in accordance with incident reporting instructions contained in DOE M 470.4-1 Chg. 1.

CHAPTER I. PROTECTION AND CONTROL PLANNING

1. CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) PROGRAM IMPLEMENTATION.

- a. To ensure the protection and control of classified information and matter, a CMPC program must be implemented to cover each Departmental element, site, and/or facility and must be tailored to achieve the protection levels that adequately address specific site characteristics and requirements, current technology, ongoing programs, and operational needs.
- b. The CMPC Program, in addition to ensuring compliance with the requirements of this Manual, must also include the following activities:
 - (1) Establishment of a point of contact with overall CMPC responsibilities for each site, facility, and program office.
 - (2) CMPC point(s) of contact must ensure the content of local CMPC training and/or briefings and awareness is commensurate with personnel responsibilities in support of the CMPC program.
 - (3) Promulgation of CMPC requirements to all affected employees.

2. PROTECTION STRATEGIES & PLANNING.

- a. Strategies for the protection and control of classified matter must incorporate the applicable requirements established in this Manual.
- b. The level of protection and resources expended on CMPC programs must be commensurate with their required effect on deterring or detecting compromise of or unauthorized access to classified matter. Protection measures should provide a graded approach, identifying each layer of protection between the adversary and the asset.
- c. Safeguards and Security Plans. The details of site protection measures for classified matter must be described in the applicable Site Security Plan (SSP) (see DOE M 470.4-1 Chg. 1).

3. DISCLOSURE AND RELEASE OF CLASSIFIED MATTER.

- a. Disclosure of Classified Information. In the event an emergency situation necessitates the intentional disclosure of classified information to individuals who are not otherwise eligible for access, the following actions must be taken if such an intentional release is required:
 - (1) Notification of Release. The following individuals must be notified as soon as possible of any emergency release of classified information to an individual or individuals who are otherwise not eligible for such access.

- (a) For RD or FRD: the Chief, Health, Safety and Security Officer; the head of the Departmental element; and the Associate Administrator for Defense Nuclear Security.
- (b) For National Security Information (NSI): the appropriate DOE line management or DOE cognizant security authority.

(2) Protection Measures.

- (a) The amount of classified information disclosed and the number of individuals to whom such information is disclosed must be limited to the absolute minimum to achieve the intended purpose.
- (b) If the information must be transmitted, it must be transmitted via approved channels if possible, or using the most secure and expeditious method if approved channels are not an option.
- (c) A description of what specific information is classified and protection requirements for the information must be provided to the recipient.
- (d) A briefing must be provided to the recipient covering requirements for not disclosing the information and a nondisclosure agreement must be signed by the recipient.

b. Release of Classified Information to Foreign Governments. To ensure the protection of classified information, the following must be met:

- (1) National Disclosure Policy Committee (NDPC). The multi-agency NDPC, of which DOE is a "Special Member," governs the export of classified U.S. military information and material to foreign governments as provided for in international agreements. To ensure uniform application of safeguards, these agreements include arrangements for the appropriate safeguarding of information and material provided to DOE. Access to classified information and material must be granted in accordance with established international agreements.

DOE has agreed to inform the NDPC of international agreements involving the sharing of all classified information, including those made under the auspices of the Atomic Energy Act. This notification must include the provisions of security agreements that apply to the shared information. DOE is also required to coordinate with the Joint Atomic Information Exchange Group before disclosing atomic information (which includes RD and FRD).

- (2) Departmental Element. The program office is responsible for ensuring DOE's compliance with national-level disclosure requirements.

- (3) Criteria for Release of Classified Information. Before releasing classified information to any foreign government, DOE must determine that furnishing the classified information will result in a net advantage to the national security of the United States. In making such a determination, the following conditions must be met:
- (a) Determination of Net Advantage to the United States. The Deputy Administrator, Defense Nuclear Nonproliferation, in coordination with the General Counsel, the Office of Health, Safety and Security, the cognizant Departmental element, and other Program Offices as necessary, must determine that furnishing classified information will result in a net advantage to the National security of the United States.
 - (b) The Deputy Administrator, Defense Nuclear Nonproliferation must consult with the Department of State and other agencies and departments, as appropriate, in making this determination.
 - (c) The disclosure must be consistent with the foreign policy of the United States toward the receiving government.
 - (d) The disclosure must be limited to information necessary to the purpose for which disclosure is made.
 - (e) The receiving government must have agreed, either generally or in the particular case, to the following stipulations.
 - 1 The receiving government must not release the information to a third party without the approval of the releasing party.
 - 2 The receiving government will afford the information substantially the same degree of protection afforded the information by the releasing party.
 - 3 The receiving government will use the information *only* for the purpose for which it was given.
 - 4 If the releasing party indicates any private rights (such as patents, copyrights, or trade secrets) are involved in the information, the receiving party will acknowledge such rights.
 - (f) In some instances, new documents may be created that contain both U.S. classified information and foreign government information (FGI). In this case, unless there is a current agreement for cooperation (for RD or FRD) or appropriate international agreement (for NSI) allowing sharing of the specific categories and

levels of U.S. classified information, the enhanced FGI cannot be returned to the originating government or international organization of governments.

- (4) Release Determination.
 - (a) Initiation and Coordination. The Departmental element responsible for the classified information to be released to a foreign government must prepare the initial request and justification. The Departmental element must coordinate with the Office of Health, Safety and Security; the Office of General Counsel; and the Office of Congressional and International Affairs for approval to release the classified information.
 - (b) Release to Non-U.S. Citizens. The release or disclosure of FGI to non-U.S. citizens must have the prior consent of the originating government, and the individual must possess appropriate security clearance and meet need-to-know requirements.
 - (c) Third-Country Transfers. The release or disclosure of FGI to any third-country entity must be coordinated through the cognizant Departmental element and Office of Health, Safety and Security and have the prior consent of the originating government if required by a treaty, agreement, bilateral exchange, or other obligation.
 - (d) Foreign Government Information Containing Unclassified United States Information. Documents containing U.S. unclassified information and FGI must be protected at the most restrictive level contained within the document.
 - (e) Returning Foreign Government Information Documents. If it is necessary to return the enhanced FGI (e.g., additional U.S. information added) to the originating government or international organization, it must be handled in accordance with paragraph 3.b above.
- (5) Transmittal of Classified Information and Classified Matter. All transmittals that involve classified information or classified matter must be made by DOE unless the contractor has prior written authorization. If the transfer involves classified information or classified matter produced by or received from another Government agency, the cognizant Departmental element must obtain approval from the agency before transmission.
- (6) Preparation and Method of Transmission. Normally, documents intended for foreign governments must be forwarded to the receiving country's embassy in the United States. The method of transmission of classified

mail to foreign countries must be approved by the Office Health, Safety and Security.

- (7) Transmittal Documentation. Copies of receipts for physical transfers must be contained in memoranda prepared by the cognizant Departmental element and maintained by the cognizant program office.
- (8) Oral Disclosure Records. Records of made and/or contemplated oral disclosures must be contained in memoranda prepared by the cognizant Departmental element and maintained by the cognizant program office.

4. TRAINING. All CMPC-related training/briefing regarding the local implementation of this Manual must be formally documented. It must also be approved by the cognizant security authority (e.g., frequency, content). (Specific training requirements, in addition to those stated in this Section, are included in DOE M 470.4-1 Chg. 1.)

- a. Each individual identified as a CMPC point-of-contact, according to Section A, Chapter I, paragraph 1.b, must receive initial training within one (1) year of appointment or as soon as training is available through the National Training Center (NTC). Other personnel may also receive the NTC-developed training.
- b. All personnel with security clearances whose classified matter responsibilities include access (potential or actual), originating, handling, using, storing, accounting for, reproducing, transmitting (including hand-carrying), destroying, and/or emergency reporting must receive CMPC training and/or briefings commensurate with these responsibilities prior to receiving access to classified matter and receive refresher training and/or briefings to ensure continued reinforcement of requirements. This training and/or briefing must be tailored to the assigned duties and responsibilities of the persons receiving the training and/or briefing.
- c. Personnel with security clearances whose job responsibilities do not meet the conditions specified in paragraph (b) above (e.g., personnel employed in maintenance, janitorial, food service, and other such activities) must receive training and/or briefings and be able to identify unprotected classified matter (e.g., by classified cover sheets and classification markings) and know the associated reporting requirements.

CHAPTER II. CLASSIFIED MATTER PROTECTION AND CONTROL REQUIREMENTS

1. GENERAL. Protection and control requirements include the following:
 - a. Prior to classification review, matter that may be classified must be protected at the highest potential classification level and category. The originator is responsible for obtaining a classification review by a derivative or original classifier if there are any questions regarding the classification of any draft document or working paper.
 - b. When information is prepared on classified information systems, the hard-copy output (which includes paper, microfiche, film, and other media) must be marked either:
 - (1) with the appropriate markings for the classification of the information as determined by a derivative classifier according to a classification review of the actual output,
 - (2) as a working paper or electronic medium to the accreditation level and category of the information system (see Chapter II, paragraph 3.p. for additional requirements that apply, regarding draft and working papers) or
 - (3) according to the marking requirements for the appropriate classification of information that has been generated by a program verified and formally approved by the Designated Approving Authority (DAA) to produce consistent results. The following factors must be satisfied when exercising this option:
 - (a) The output that will be produced must be fully defined and documented. The DAA must formally approve this documentation and must ensure that any subsequent output marked according to this option completely matches the planned and actual output for which the Classification Officer determined the classification level (and category if Restricted Data [RD] or Formerly Restricted Data [FRD]),
 - (b) The Classification Officer must review the fully defined output and must determine the correct classification level (and category if RD or FRD) for the information contained in the output, and
 - (c) All output must be marked with the correct classification level (and category if RD or FRD) as determined by the Classification Officer.
 - c. When matter must be sent outside the office of origin for a classification review and determination, it must be marked "DRAFT—Not Reviewed for

Classification.” To preclude marking every page of a document being transmitted for classification review, it should have a “Document Undergoing Classification Review” cover sheet that is marked with the highest level and most restrictive category of information the originator believes is contained in the document.

- d. Access to classified matter in an emergency involving an imminent threat (explosion, fire, etc.) to life or defense of the homeland may be provided to individuals who are not otherwise routinely eligible for access to classified matter. If an emergency is life-threatening, the health and safety of individuals takes precedence over the need to protect classified matter from disclosure. Examples of such releases include providing law enforcement personnel with classified information concerning an improvised nuclear device found in a public place, sharing a classified DOE evaluation of the viability of a nuclear threat message with local emergency response personnel, or providing an attending physician with classified details about nuclear materials at a site to assist in the emergency treatment of a patient.
 - (1) Protecting Classified Matter in Emergency Situations. DOE Cognizant Security Authority (DOE CSA)-approved procedures must be developed. These procedures must describe the actions (i.e., notifications, alternative storage, and protection methods) to be taken at the time of the emergency.
 - (a) Every attempt must be made to minimize access by uncleared emergency response personnel to only those areas directly affected by the emergency situation.
 - (b) All unsecured classified matter must be accounted for following the emergency.
 - (c) Secure storage repositories must be inspected on return to the facility to ensure they have not been compromised.
 - (2) Emergency Evacuation Drills/Tests. Emergency evacuation drill/test procedures must include protection requirements and Cognizant Security Authority (CSA)-approved procedures for protecting all classified matter from unauthorized access.
 - (3) Reporting Requirements. Report in accordance with incident reporting instructions contained in DOE M 470.4-1 Chg. 1.
2. CLASSIFIED MATTER IN USE. Classified matter in use must be constantly attended by or under the control of a person possessing the proper security clearance and need to know.
3. MARKING. All classified matter, regardless of level and category, must be marked to ensure information is appropriately protected to prevent inadvertent disclosure. Classified matter must be reviewed and brought up to current marking standards whenever it is

released by the current holder (“current holder” may be defined as an individual, specific office, or ad-hoc working group [AHWG]) or removed from archival storage. Marking requirements for foreign government information (FGI) are found in 9.b. below. Marking examples can be found in the DOE Marking Handbook (see http://www.pnl.gov/isrc/pdf/doe_marking_handbook_2006.pdf).

a. General.

- (1) Requirements. Classified matter, regardless of date or agency of origin, must be marked to indicate at least the classification level and category (if RD or FRD).
 - (a) Classified NSI documents that were created after April 1, 1996, and that lack appropriate current markings including declassification on a date or event, classification basis, or classifier’s name, must be reviewed by a derivative classifier to ensure the classification level and category are still correct and then re-marked to bring them up to current marking requirements.
 - (b) Classified matter retained for litigation or for official archival purposes, including classified matter transferred during site closure, need not be brought up to current marking standards.
 - (c) DOE M 475.1-1B, *Identifying Classified Information*, provides requirements for reviewing and marking documents with obsolete markings.
- (2) Markings. All classification markings must be distinguishable from the document text. The overall classification level (i.e., Top Secret, Secret, or Confidential) of a document must be marked on the top and bottom of the cover page (if any), the title page (if any), the first page of text, and the outside of the back cover or last page of text. The classification level and category (if RD or FRD) must be clearly marked on all other (non-document) classified matter if possible. Otherwise, alternative marking methods must be used to identify the overall classification level and category (if RD or FRD). When marking the level or category is not practical, written notification must be furnished to all recipients. The originator is responsible for ensuring that classified matter is marked in accordance with this Manual. DOE M 475.1-1B contains additional marking requirements beyond the requirements contained in this Manual.

All interior pages of documents must be marked top and bottom with either:

- (a) The overall classification level and category (if RD or FRD) for the entire document, or

- (b) The highest classification level and category (if RD or FRD) of all information on that page; or with appropriate unclassified marking (e.g., Unclassified, OUO, UNCI) if there is no classified information on that page.
 - (3) Unique Identification Numbers. Classified matter required to be in accountability, as defined in Section A, Chapter II, paragraph 5, must have a unique identification number.
- b. Originating Organization and Date. The name and address of the organization responsible for preparing the document and the date of preparation must appear on the first page of all classified documents.
- c. Classification Categories. The three classification categories are RD, FRD, and NSI. Classified matter containing only NSI is *not* marked with a NSI admonishment.
 - (1) If the document contains RD or FRD information, the appropriate admonishment information must be marked on the first page of the document, whether cover page, title page, or first page of text and appear in the lower left corner.
 - (2) RD or FRD documents generated prior to July 9, 1998, are not required to be re-marked to indicate the category on each page containing RD or FRD information unless they are sent outside the office of origin or holder for other than archiving purposes.
- d. Mixed Levels and Categories. When classified matter contains a mix of information at various levels and categories that causes the document to be marked at an overall level and category higher than the protection level required for any of the individual portions, a marking matrix may be used in addition to other required markings. This would allow an individual with a lower access level, such as an "L" cleared employee, to be given access to a document that they might not otherwise have been authorized access to if the document was only marked at the highest overall classification level and category. (For example, a document that contains Confidential RD and Secret NSI would be required to be marked as Secret RD, the highest level and most restrictive category. None of the information in the document is Secret RD). However, this may not be interpreted to authorize any individual to gain access to information that exceeds their security clearance, formal access approvals, and need to know.

If the marking matrix is used, the following marking, in addition to other required markings, must be placed on the first page of text. The marking should appear on the lower right corner near the classifier information marking. If the derivative classifier places this marking on the document at the time of the classification decision, there is no need to indicate the name and title of the derivative classifier on the mixed level and category marking.

This document contains:

Restricted Data at the (e.g., *Confidential*) level.
Formerly Restricted Data at the (e.g., *Secret*) level.
National Security Information at the (e.g., *Secret*) level.

Classified by: *Name and Title*

- e. Components. When components of a document are to be issued or used separately, each major component must be reviewed and marked as a separate document. Components include annexes or appendixes, attachments, and major sections of a report. If an entire major component is unclassified, "Unclassified" must be marked at the top and bottom of the first page and a statement included (e.g., "All portions of this [annex, appendix, etc.] are Unclassified"). When this method of marking is used, no further markings are required on the unclassified component. Documents transmitted with a letter of transmittal are discussed in paragraph 3.o. below, Transmittal Documents.
- f. Unclassified Matter.
 - (1) Unclassified matter need not be marked unless it is essential to convey one of the following conditions:
 - (a) The matter has been reviewed for classification and does not contain classified information; or
 - (b) The matter has been properly declassified.
 - (2) If unclassified matter is marked, the Unclassified marking must be placed on the top and bottom of the front cover (if any), title page (if any), and first page of text.
- g. Portion Marking.
 - (1) NSI documents dated after April 1, 1997, must be portion marked.
 - (2) Documents containing RD or FRD should not be portion marked; however, if portion-marked, markings must be consistent with this Chapter.
 - (3) Portion markings must include any applicable caveats. Each section, part, paragraph, graphic, figure, subject/title, or similar portion of any such document must be accurately marked to show:
 - (a) the classification level, category (if RD or FRD), and caveat (e.g., S/RD, S/FRD, C/RD, C/FRD, S, TS, S/NOFORN, etc.) or
 - (b) that it is unclassified [e.g., (UCNI), (OUO), or (U)].

- (4) Page changes to NSI documents dated after April 1, 1997, must be portion marked. Additionally, any NSI document that becomes active (i.e., when it is released by the current holder, which may be defined as an individual, specific office, or AHWG, or removed from archival storage) must be portion marked with the appropriate classification level, caveat, or unclassified.
 - (5) Portions of U.S. documents containing Foreign Government Information (FGI) must be marked to reflect the foreign country of origin and appropriate classification level (e.g., U.K.-C, indicating United Kingdom-Confidential). FGI must be indicated in lieu of the country of origin if the foreign government indicates it does not want to be identified.
 - (6) Classification by Association or Compilation. DOE M 475.1-1B contains portion marking and other requirements for classified matter determined to be classified by association or compilation.
- h. Subjects and Titles. Titles must be marked with the appropriate classification (level; category if RD or FRD; and other applicable caveats) or control symbol or “U” if unclassified and placed immediately after the item.
- i. Classifier Markings. Classifier marking requirements can be found in DOE M 475.1-1B.
- j. Caveats and Special Control Markings. Caveats and special control markings are placed on documents to identify special handling or dissemination requirements or to assist in describing the type of information involved or who distributed or originated the information. Caveats and special control markings and any related admonishment statements or notices should be placed above the category admonishment statement, if any, on the lower left corner of the first page (cover page, if any; title page, if any; or first page of text) and in portion markings, when required.
- k. Re-marking Upgraded, Downgraded, and Declassified Matter. Requirements for marking upgraded, downgraded, or declassified matter are contained in DOE M 475.1-1B.
- l. Re-marking Automatically Declassified Matter. Matter marked for automatic declassification must not be re-marked unless it has been reviewed and determined by an Authorized Derivative Declassifier not to contain classified information (see DOE M 475.1-1B).
- m. Classified Matter Not Automatically Declassified. For requirements see DOE M 475.1-1B.

- n. File Folders and Other Containers. File folders and other items containing classified matter, when removed from secure storage repositories, must be conspicuously marked to indicate the highest classification level of their contents.
- o. Transmittal Documents. The first page of a transmittal document must be marked with the highest level and most restrictive category (if RD or FRD) of classified information being transmitted and with an appropriate notation to indicate its classification when the enclosures are removed.
- p. Working Papers and Drafts. Classified working papers and drafts are considered to be interim production stages toward the generation of a final document.
 - (1) Hard copies of working papers and drafts must contain the following markings:
 - (a) the date created;
 - (b) the highest potential overall classification level of the draft or working paper at the top and bottom of the outside of the cover page (if any), on the title page (if any), on the first page of text, and on the outside of the back cover or last page. Each interior page of a classified document must be marked at the top and bottom with the highest potential classification level of that page (including unclassified) or the overall classification of the document;
 - (c) the overall category (if RD or FRD) of the draft or working paper must be marked on the cover page (if any), title page (if any), or the first page of text. The category marking is not required on draft and working paper interior pages that contain RD or FRD information;
 - (d) the annotation “Working Paper” or “Draft” must be marked on the first page of text; and
 - (e) any applicable caveats or special markings must be annotated on the cover page (if any), title page (if any), or the first page of text.
 - (2) Markings prescribed for a finished document must be applied when a draft or working paper meets any of the following requirements:
 - (a) released by the originator outside the activity, office, or AHWG;
 - (b) Top Secret retained for more than 30 days from the date of origin;
 - (c) Secret or Confidential retained for more than 180 days from the date of origin; or
 - (d) it will no longer be revised.

- (3) Classified documents that are updated on a frequent basis, commonly referred to as “living” documents (e.g., documents that are part of an ongoing experiment or study) may be considered as originating on each date they are changed. Local procedures must document specific techniques to demonstrate that working papers and drafts are “living” documents (e.g., a sheet attached to the front of the document that gives the number of pages or date of the last change is an example of such a technique).
 - (4) See Section A, Chapter II, Paragraph 1.c. for requirements for documents undergoing classification review.
- q. Redacted Documents. Methods used to strike out classified information before release to persons not authorized access to the deleted information must completely obliterate the classified text, figures, etc., to prevent any form of recovery that might compromise the information. DOE M 475.1-1B contains additional redaction requirements.
- r. Other Government Agency (OGA) Not Conforming to DOE Requirements. As a rule, documents received from OGAs and foreign governments that have not been marked to conform to DOE requirements do not need to be re-marked. However, all documents received must clearly indicate a classification level and category (if RD or FRD). The sender must be contacted to resolve any marking questions.
- s. Cover Sheets. Cover sheets must be applied to all classified documents when they are removed from a secure storage repository. (Reference: Standard Forms 703, 704, and 705)
- 4. MARKING MATERIAL.
 - a. Requirements. The classification level and category (if RD or FRD) must be conspicuously marked on all classified material. When marking is not practical, written notification of the markings must be furnished to recipients.
 - b. Caution. Before initiating any new marking policies, it is necessary to coordinate with the production engineers. War reserve and configuration control requirements mandate strict control over what is done to specific materials—markings cannot violate these rules. Any alternative markings under consideration must be compatible with the material being marked.
 - c. Exempted Markings. Because the classifier’s annotation and origination date are maintained on the drawing specifications, these markings are not required on each piece of classified material. Other markings such as originator identification and unique identification number (accountable material only) do not apply because of the nature of the material.

5. CONTROL SYSTEMS AND ACCOUNTABILITY.

- a. General. Control systems must be established and used to prevent unauthorized access to or removal of classified information. Accountability systems must provide a system of procedures that provide an audit trail. Accountability, as defined below, applies regardless of the physical form of the matter (e.g., electronic, paper, or parts).
- b. Accountable Matter. The following are types of accountable matter:
 - (1) Top Secret matter,
 - (2) Secret matter stored outside an LA (or higher),
 - (3) Any matter that requires accountability because of national, international, or programmatic requirements such as the following:
 - (a) classified computer equipment and media supporting the Nuclear Emergency Support Team (NEST) and Accident Response Group (ARG) operations and similar elements;
 - (b) national requirements such as cryptography and designated COMSEC;
 - (c) international requirements such as North American Treaty Organization (NATO) ATOMAL, designated United Kingdom documents, or other FGI designated in international agreements;
 - (d) designated SAPs; and
 - (e) Sigma 14.
 - (4) Classified Removable Electronic Media (CREM), which is required to be marked as S/RD or higher classification, or which is otherwise accountable (see paragraphs 5.b.(2) and (3) above). Each piece of accountable CREM (ACREM) must remain in accountability until verification that none of the information that requires the CREM to be accountable can be retrieved or recovered from that piece of CREM. Only National Security Agency-approved methods or other officially approved methods that comply with DOE cyber security policy may be used to determine whether information is recoverable from ACREM. Any such approved methods or criteria must be performance-tested as necessary to ensure that unauthorized access to classified information does not occur.
- c. Accountable Classified Removable Electronic Media (ACREM) Custodians.
 - (1) At least one appointed and trained ACREM custodian and alternate ACREM custodian must be assigned for each secure storage repository or

file cabinet used to store ACREM. If more than one custodian and one alternate custodian are assigned, the number of individuals assigned to these positions must be identified and justified through documented cognizant security authority-approved procedures and must be kept to the minimum number necessary based on operational need and associated risk.

- (2) These appointed individuals are responsible and accountable for ACREM, all accountability records, and other duties outlined in cognizant security authority approved local procedures that must include, but are not limited to: a documented ACREM check out and transfer process implemented to record all ACREM transfers between ACREM custodians, alternate ACREM custodians, and users. This process must be performance-tested to ensure its effectiveness.
- d. Control Stations. Control stations must be established to maintain records, accountability systems, access lists (when required), and control classified matter (including facsimiles) received by and/or dispatched from facilities. Control station operators must maintain accountability systems for accountable matter. A defined and operated ACREM accountability process may function as a control station.
 - e. Accountability Records. Accountability records are required when accountable matter is originated, reproduced, transmitted, received, destroyed, permanently buried, or changed in classification. All sites must develop procedures to ensure that all accountable matter has been entered into accountability systems. At a minimum, accountability records must indicate the following information for each item of accountable matter. If accountable matter is received from another agency and lacks a unique identification number, one must be assigned.
 - (1) Date of the Matter. The date the matter was originated or created. For documents, this term means the date the document was finalized.
 - (2) Brief Description of the Matter (unclassified, if possible). Examples include the unclassified title (if a document) or description (if material). It may also be helpful to describe the form of the matter (e.g., a document, magnetic medium, microform, drawing, photograph, or photographic negative). If a title or description is classified, an unclassified descriptor should be used to prevent the accountability records system from becoming classified.
 - (3) Unique Identification Number. This could be a unique document number (if a document) or serial number (if material). Unique identification numbers may be provided by creating a totally new number for each individual document, including copies, or by adding the copy and series to the old base number when reproducing accountable documents. The key

point is to ensure that each document, whether an original or a reproduction, has some kind of unique number associated with it.

- (4) Classification Level (and Category, if RD or FRD) and Caveats. Classification level, category (if RD or FRD), and additional handling caveats, if any, of the matter must also be indicated.
- (5) Number of Copies and Disposition. The number of copies of a document (including the original) generated during either origination or reproduction, the disposition of each copy (e.g., destruction, downgrading, declassification, dispatch outside the facility, or incorporation into another accountability record), and the date of disposition. The term “disposition” varies in meaning as follows regarding:
 - (a) origination, transmission, receipt, and reproduction, “disposition” means the offices or activities where the matter was distributed;
 - (b) destruction, “disposition” means the organization where the matter was destroyed and by whom; or
 - (c) change of classification, “disposition” means which office or activity performed the change of classification and which offices or activities have copies of the matter.
- (6) Originator Identification. The organization name and address of the originator. For material, this information is found in the associated paperwork.
- (7) Authority for Contractor Retention. Contract or other written retention authority that authorizes the matter to be in the possession of a contractor. This authorization can be either a letter of authorization or a contract reference to the authorization to retain classified matter. A copy of this authorization should be maintained with the accountability records and should be readily available to facilitate compliance disposition reviews.
- (8) Date Received (if applicable). The date the transmitted matter arrived.
- (9) Activity from Which the Matter was Received (if applicable). The office or activity name and address from which matter was transmitted to the recipient.
- (10) Responsible Individual. The individual who checked it in and/or out (who has personal responsibility for it).

f. Accountable Material.

- (1) General. Accountability procedures must be approved by the cognizant security authority.

- (2) Exemptions. When they are *not* applicable, the following items are exempt from inclusion in the material accountability records:
 - (a) matter date;
 - (b) number of copies; and
 - (c) date and disposition of reproduction.
- (3) Requirements. The material accountability system must provide a description of each type of item, the classification level and category (if RD or FRD), the number of items of each type, and scheduled inventories. Part numbers and serial numbers should be used, when available, as a unique number or to identify the types of material. Where applicable, the production cycle and production control procedures can be used to facilitate the conduct of all inventories of accountable material.

g. Inventory.

- (1) Frequency.
 - (a) All ACREM must be inventoried and all results documented on a recurrent basis. All discrepancies between ACREM records and the verified locations and status of all ACREM, must be identified and reconciled (examples of status include possessed by an identified individual, stored, or destroyed).
 - 1 The current and previous individual assigned control/possession of all ACREM, according to their assigned custodians and users, must be documented and available at any given time within record retention periods. Inventories and resolution of discrepancies must be used to validate that local ACREM custodians, alternate custodians, users, and procedures are meeting this performance requirement;
 - 2 The baseline required frequency of the recurrent ACREM inventories is monthly (no longer than 31 calendar days between inventories). However, the DOE cognizant security authority may increase the time between inventories up to a maximum of six months. The DOE cognizant security authority's decision to decrease inventory frequency must be based on a documented determination that doing so will result in no unacceptable increased risk to the ACREM. Factors to consider in making this determination include:

- a the amount of ACREM;
 - b the number of formally appointed ACREM custodians and alternate custodians;
 - c ACREM usage levels;
 - d strength of the local Classified Matter Protection and Control Program;
 - e characteristics of the local facilities, equipment and procedures; and
 - f past performance in managing ACREM.
- 3 Inventories are not required for ACREM maintained in a locked file cabinet or General Services Administration (GSA) approved security container that is located in a vault or a VTR, or is maintained in security containers with XO-Series locks, and the container has not been accessed since the last inventory. However, time between inventories must not exceed 1 year (365 calendar days) for any ACREM.
- (b) National Nuclear Security Administration's (NNSA) Nuclear Emergency Search Team (NEST), Accident Response Team (ARG), and similar elements' classified computer equipment and media (non-ACREM) must be inventoried at least once a month by two individuals. In addition, DOE cognizant security authorities must develop deployment and redeployment checklists for all ARG, NEST, and similar elements that include procedures for inventorying accountable equipment both before and after a deployment.
- (c) All other accountable matter must be inventoried no less frequently than every 12 months.
- (2) Inventories must consist of a physical comparison of each item against the current inventory listing. Discrepancies must be resolved, if possible using the previously reconciled inventory and receipts, transfers and destruction records. Each item listed in an accountability record must be verified visually.
- (3) Reports. Any unresolved discrepancies between the items found to be present and the inventory list must be reported and dealt with according to DOE policy and requirements for reporting incidents of security concern (see DOE M 470.4-1 Chg. 1).

- h. Master Files and Databases. Master files and databases created in central data processing facilities to supplement or replace Top Secret records are *not* authorized for disposal under National Archives and Records Administration's General Records Schedule 18. These files must be scheduled on an SF 115, *Request for Records Disposition Authority*.
 - i. Automated Accountability Systems and Electronic Receipting.
 - (1) Automated Accountability Systems. Automated accountability systems must:
 - (a) be approved by the DOE cognizant security authority;
 - (b) implement the requirements under paragraph 5.e. above; and
 - (c) provide security controls to ensure that no unauthorized changes are made to system records.
 - (2) Electronic Receipting. Electronic receipting systems are approved as long as the following conditions are met. The system:
 - (a) is approved by the DOE cognizant security authority;
 - (b) provides identification of both the individual and the document disposition; and
 - (c) provides adequate security controls to ensure that no unauthorized changes are made to the system record.
6. REPRODUCTION.
- a. General.
 - (1) Cognizant security authority-approved procedures must be established for the reproduction of classified matter. Reproduction of classified matter must be limited to the minimum number of copies consistent with operational requirements and any other pertinent reproduction limitations. Local procedures should address the issue of controlling the number of copies of classified documents.
 - (2) Reproduction must be accomplished by authorized persons who know the procedures for classified reproduction and only in the performance of official or contractual duties.
 - (3) Classified documents may be reproduced without originator approval except when they contain markings that limit reproduction.

- (4) To restrict reproduction of a classified document, consider one of the following techniques.
 - (a) For intelligence documents only, the Originator Controlled (ORCON) caveat marking may be used to restrict reproduction to that allowed by the originator.
 - (b) Originators of non-intelligence documents who wish to prevent unlimited copying of a classified document may use the markings restricting duplication without originator approval.
 - (5) When any of the data that reside on a piece of ACREM (source media, in this case) is moved to, or reproduced on, another piece of media, the receiving media immediately becomes (or remains) accountable because it must be assumed to contain that which made the source media accountable, until proven otherwise and approved by the DOE Cognizant Security Authority (DOE CSA).
- b. Equipment. Classified matter must be reproduced on equipment specifically approved and designated for this purpose to ensure minimal risk of unauthorized disclosure or access. To the greatest extent possible, this equipment must be located within LAs, PAs, EAs, or MAAs.
- (1) Access to Machines. Classified copying must not be performed in the presence of individuals lacking the proper security clearances or need to know.
 - (2) Approval. Ensure all machines to be used for reproducing classified documents are approved in accordance with local procedures and cyber security policy.
- c. Documents Received From Outside Agencies. Outside agency documents may be reproduced in accordance with the same rules and restrictions that exist for DOE documents. Therefore, unless specific instructions to the contrary accompany the documents, they may be reproduced. For example, National Security Council (NSC) documents will have a copy restriction notice; therefore, NSC documents will be reproduced only with the permission of the originator.

7. RECEIVING AND TRANSMITTING CLASSIFIED MATTER.

- a. General. Classified matter must be transmitted only in the performance of official or contractual duties. If the transmission is not required by the specific terms of the contract or required for performance of the contract, contractors must obtain written authorization from the DOE cognizant security authority before transmitting classified matter outside the facility. Before transmitting classified matter, the sender must ensure:

- (1) The recipient has the appropriate security clearance, has any required programmatic or special access approval, and meets the need-to-know criteria.
 - (2) An approved classified address has been identified and used for the appropriate method of transmission, e.g., mailing, shipping, or overnight delivery.
- b. Receiving. When classified matter is received at a facility, the following controls must apply (also see paragraph 7.d. below):
 - (1) Classified matter must be delivered to personnel designated to receive it at a control station with the inner envelope unopened. Procedures must be established to ensure that when classified matter is not received directly by the designated control station (regardless of the type of mail system), the inner container remains unopened.
 - (2) The package must be examined for evidence of tampering and the classified contents checked against the receipt (if provided). Evidence of tampering must be maintained and reported promptly to the cognizant security authority. If the matter was received through the U.S. Postal Service, the appropriate U.S. Postal Inspector must also be notified promptly. Discrepancies in the contents of a package must be reported immediately to the sender. If the package (or container) is in order and includes a receipt, the receipt must be signed and returned to the sender.
- c. Packaging. Classified matter to be transmitted outside a facility must be double-wrapped (enclosed in opaque inner and outer containers) except as specified below. The contents of the package or shipment must be securely packaged to meet DOE and the applicable transporting agency's requirements, i.e., the U.S. Postal Service, for transmission.
 - (1) Envelopes and Similar Wrappers. All classified information physically transmitted outside facilities must be enclosed in two layers, both of which provide appropriate protection and reasonable evidence of tampering and which conceal the contents. The inner enclosure must clearly identify the classified address of the sender and the intended recipient, the highest overall classification level, and category (if RD or FRD), of the contents, and any appropriate warning notices. The outer enclosure must be the same except that no markings to indicate that the contents are classified must be visible. Intended recipients must be identified by name only as part of an attention line.
 - (2) Other Containers. The outer container must maintain the integrity of the inner container.

- (a) As long as the item is enclosed in a double container, the matter may be wrapped or boxed in paper, wood, metal, or a combination thereof.
- (b) If a locked briefcase is used to hand-carry classified matter of any level, the briefcase may serve as the outer container. A briefcase must not serve as the outer container for travel aboard public transportation.
- (c) The outer container must be addressed to a classified address, return-addressed to a classified mailing address, and sealed, with no markings to indicate the contents are classified.
- (d) If specialized shipping containers, including closed cargo transporters, are used for transmitting classified matter, the shipping container can be considered the outer container.

(3) Equipment Components.

- (a) If the classified matter is an internal component of a packaged item of equipment with an outside shell or body that is unclassified and that completely shields the classified internal component from view, the shell or body may be considered the inner container. If the shell or body is used as the inner container the address and return address may be omitted.
- (b) If the classified matter is an inaccessible internal component of a bulky item of equipment, such as a missile, that cannot be reasonably packaged, no inner container is required and the outside shell or body may be considered the outer container if it is unclassified.

d. Offsite Transmittal and Receipts. When transmitting secret or accountable classified matter outside site/facilities by any method, a receipt must be used. Receipts must identify the classified contents and the names and addresses of both the sending and receiving facilities. Receipts must not contain classified information. If not practical, the receipt may be sent to the recipient with the required advance notification of shipment or may be hand-carried. When classified matter is transmitted by courier, DOE F 5635.3, *Classified Document Receipt*, or a receipt comparable in content must be used.

- (1) Receipt Information. The receipt must be prepared in triplicate and remain unclassified when completed. Two copies of the receipt must be placed in the inner container with the matter (except as noted above) and sent to the intended recipient. The third copy must be maintained by the sender until the original is signed and returned. The receipt must contain the following information:

- (a) full names of the sender and the recipient;
 - (b) unclassified address of the sender, unless the receipt contains classified information and a classified mailing address for the sender is required;
 - (c) classified address of the recipient;
 - (d) description of the classified matter (e.g., title or other means);
 - (e) date of the matter;
 - (f) classification of the matter; and
 - (g) unique identification number, if accountable.
- (2) Multiple Recipients. A separate receipt must be completed for each recipient regardless of the number of items for each recipient.
 - (3) Facsimile Transmission. Individuals transmitting classified information through facsimile systems must confirm and document receipt with the intended recipient.
 - (4) Returning Receipts. The recipient of any classified matter that contains a receipt must complete the receipt and return it to the sender as soon as possible, but no longer than 30 days following receipt of matter. A copy of the receipt must be maintained with the control station records.
 - (5) Receipt Tracking. Procedures should be established for both tracking the return of receipts and the actions required if receipts are not returned.
 - (6) Electronic Receipting System. Any electronic receipting system must be approved by DOE cognizant security authority. The system must be able to identify the custodian of the classified matter or the disposition, and ensure signature authentication.
- e. Classified Addresses.
- (1) Classified addresses must be verified through the Safeguards and Security Information Management System (SSIMS) or the Defense Security Service (DSS). If not in either system, a new classified mail channel must be established. See DOE M 470.4-1 Chg. 1 for additional requirements.
 - (2) Hard-copy printouts of the SSIMS or DSS classified addresses can only be used to validate approved classified addresses for 30 calendar days from print date.

- f. Transmittal and Receipt within Facilities. Classified matter may be transmitted within a facility without single or double-wrapping provided adequate security measures are taken to protect the matter against unauthorized disclosure.
 - (1) Although double-wrapping is not required for classified matter transmitted within a facility, the transmittal method should dictate the most suitable method of protection.
 - (2) The matter may be transmitted by approved electronic means. When using this method, both the transmitting and receiving systems must be approved for the classification level and category of the information to be transmitted. Facilities also must have an approved security plan and procedures for transmitting the information by electronic means.
- g. Transmitting Confidential Matter Outside of Facilities.
 - (1) Confidential matter must be transmitted by any of the following methods or any method approved for the transmission of Secret or Top Secret matter.
 - (2) U.S. Postal Service Certified Mail is authorized within the 50 States, the District of Columbia, Puerto Rico, and U.S. territories or possessions. A return mail receipt is not required; however, if the parcel does not arrive at the appointed destination, action may be taken to obtain a receipt. A return receipt may be requested before or after delivery for all Certified Mail and Registered Mail. NOTE: OGAs may use First Class Mail; but First Class Mail is not authorized for DOE.
 - (3) DOE and DOE contractors may receive Confidential matter from OGAs through U.S. Postal Service Express Mail. The use of the U.S. Postal Service Express Mail is not permitted for the transmission of Confidential matter by DOE and DOE contractors.
- h. Transmitting Secret Matter Outside of Facilities.
 - (1) Secret matter must be transmitted by one of the following ways or by any method approved for the transmission of Top Secret matter.
 - (2) Postal/Mail Services.
 - (a) U.S. Postal Service Registered Mail is authorized within the 50 States, the District of Columbia, and Puerto Rico. A return receipt is not required for U.S. Postal Service Registered Mail.
 - (b) U.S. Registered Mail through Army, Navy, or Air Force Postal Service facilities, provided approval is obtained from the Office of Health, Safety and Security and information does not pass out of U.S. citizen control or through a foreign postal system. This

method may be used to transmit Secret matter to and from U.S. Government or U.S. Government contractor employees or members of the U.S. armed forces in a foreign country. A return mail receipt is not required.

- (c) Canadian registered mail with registered mail receipt to and between the United States Government and Canadian Government installations in the 50 States, the District of Columbia, and Canada.
 - (d) DOE and DOE contractors may receive Secret matter from OGAs through U.S. Postal Service Express Mail. U.S. Postal Service Express Mail is not permitted for the transmission of Secret matter by DOE and DOE contractors.
 - (e) Approved commercial express service organizations in accordance with the provisions contained in paragraph 7.k. below.
 - (f) Approved common carrier services with escorts who possess the appropriate security clearance in accordance with paragraph 7.l. upon approval by the cognizant security authority.
- i. Transmitting Top Secret Matter Outside of Facilities. Top Secret matter must be transmitted in one of the following ways after approval by the DOE cognizant security authority:
 - (1) by the Defense Courier Service,
 - (2) the Department of State Courier System if outside the United States and its territorial areas,
 - (3) over approved communications networks (see DOE O 200.1, *Information Management Program*, dated 9-30-96, for requirements), or
 - (4) by individuals authorized to hand-carry Top Secret matter in accordance with paragraph 7.j. below.
- j. Hand Carrying. The following requirements apply to hand-carrying classified matter; however, the requirements identified in paragraph 7.l. below, also apply to hand-carrying bulk documents.
 - (1) Local procedures must be developed describing the process for obtaining approval (including approval authority) to hand-carry outside of a site/facility and for providing notification when removing classified matter from the facility. Local hand-carry procedures must be approved by the cognizant security authority.
 - (2) A record/receipt of the classified matter must be made before departure, retained by the employee, and inventory must be made of the matter for

which the employee was charged. The record should contain the following information:

- (a) subject or title (unclassified, if possible);
 - (b) date of the matter;
 - (c) date the matter was removed from the facility;
 - (d) signature of the person removing the matter; and
 - (e) date the matter was returned; or date and recipient's name and organization from receipt for matter that was transferred to another individual.
- (3) The removal of classified matter from approved facilities to private residences or other unapproved places (e.g., hotel or motel rooms) is prohibited.
- (4) Contingency plans for delayed arrival must cover alternative protection and storage procedures, reporting requirements, and be approved by the cognizant security authority.
- (5) Classified matter may be hand-carried outside the United States, provided the following conditions are met.
 - (a) The traveler must possess appropriate security clearance and a diplomatic passport. Diplomatic passports can only be issued to Federal personnel attached to a mission or embassy as a tenant or performing a mission under the auspices of the Department of State.
 - (b) The traveler must obtain written authorization from the cognizant Departmental element.
- (6) Requirements for security screening of classified matter at airports are established by the Transportation Security Administration (TSA).
- k. Approved Commercial Express Service Organizations. The use of commercial express service organizations for transmitting classified matter is restricted to emergency situations and the matter must be delivered to and secured at the receiving location the next calendar day.
 - (1) General. At a minimum, the sender must ensure that the following conditions are met.
 - (a) The use of the express service organization has been approved by the sender's DOE CSA and an address for receiving deliveries

from the express service has been input into SSIMS for the receiving organization.

- (b) The address selected for the overnight/commercial express service cannot be greater than five lines, *cannot* be a post office box, and must be a street address.
- (c) The intended recipients must be notified 24 hours in advance (or immediately if transit time is less than 24 hours) of the proposed shipments and arrival dates.
- (d) All packages are double-wrapped before being inserted into the packaging provided by the commercial express service organization.
- (e) In accordance with packaging requirements, commercial express service packages must not be identified as classified packages.
- (f) The properly wrapped packages are hand-carried to the express mail dispatch center or picked up from a control station in sufficient time to allow for dispatch on the same day.
- (g) Commercial express carrier drop boxes must not be used for classified packages.
- (h) Facilities should include specific details regarding the use of package tracking in local procedures. The commercial express carrier may be contacted for details regarding packaging requirements.

- (2) Problems. Problems with the delivery of classified matter via commercial express service delivery must be reported in accordance with reporting of security incidents (see DOE M 470.4-1 Chg. 1).

- I. Common Carrier Services. Common carrier services include all modes and means of transport (e.g., air, rail, vehicular, and intercity messenger services) excluding express service organizations. The following requirements apply to the use of such commercial services as well as for bulk shipments of classified matter.

- (1) General.

- (a) The contents must be securely packaged to meet DOE and Department of Transportation requirements for transmission.
- (b) Seals or other tamper-indicating devices approved by the cognizant security authority must be placed in a manner to show evidence of tampering on all freight and/or bulk shipments other than overnight commercial express packages. Seals must have serial numbers,

which must be entered on bills of lading or other shipping papers. Seal numbers must be verified by the consignee upon arrival of a shipment.

- 1 Whenever practical, combination padlocks meeting Federal Specification FF-P-110, Padlock, Changeable Combination must be used to secure closed cargo areas of vehicles, vans, and railroad cars.
- 2 Shipments of Secret or Confidential matter received at common carrier terminals must be picked up by the consignee on the day of arrival unless the carrier provides continuous protective service to the address of the consignee under locally approved procedures.

(2) Assurances and Notifications.

- (a) Notification of shipments must be transmitted to the consignee before departure with 24-hour advance notice (or immediately upon dispatch if within 24 hours) to enable proper handling at the destination. At a minimum, the notification must include the nature of the shipment, means of shipment, number of seals, anticipated time and date of arrival, and requested notification if not received by a specified time.
- (b) The consignee must advise the consignor of any shipment not received within 24 hours after the estimated time of arrival furnished by the consignor or trans-shipping activities personnel. Upon receipt of such notice, the consignor must immediately begin tracing the shipment.

(3) Protective Measures. Protective measures for Departmental security shipments are as follows.

- (a) Sufficient personnel with appropriate security clearance must be tasked for a specific movement assignment to ensure continuous protection of the matter being transported.
- (b) At a minimum, the common carrier service must be required to provide the following security services.
 - 1 surveillance by an authorized carrier employee with appropriate security clearance when the classified matter is outside the vehicle;
 - 2 a tracking system that ensures prompt tracing of the shipment while en route; and

3 an alarmed or guarded storage area with immediate response by a carrier employee, commercial guard, or police officer when storage is required.

- (c) When shipments are transported by rail or motor vehicle, personnel escorting the shipments must keep the shipment car(s) under observation, maintain continuous vigilance for conditions or situations that might threaten the security of the cargo, and take appropriate actions as circumstances require. During stops or when practical and time permits, personnel escorting shipments must check the cars, container locks, and/or tamper-indicating devices.

8. DESTRUCTION.

- a. Local procedures must be established for the ongoing review of classified holdings (e.g., multiple copies, obsolete matter, classified waste) to reduce volume to the minimum necessary.
- b. If under a court order prohibiting destruction, special destruction procedures may be required. Under such circumstances, all destruction activities must be conducted in accordance with guidance provided by the DOE Office of General Counsel and the appropriate records management organization.
- c. Classified matter must be destroyed beyond recognition to preclude subsequent access to any classified information. Electronic storage media (ESM) must be destroyed in accordance with the DOE cyber security directives. Destruction techniques include burning, shredding, pulping, melting, mutilating, pulverizing, or chemical decomposition. The following additional requirements must be satisfied when classified matter is destroyed.
 - (1) The DOE cognizant security authority must approve the use of public destruction facilities and any other alternative procedures.
 - (2) If classified matter cannot be destroyed onsite, it may be destroyed at a public destruction facility. If a public destruction facility is used, an appropriately cleared individual must ensure the destruction occurs on the same day it leaves a cleared facility and that the destruction is properly witnessed. A record of dispatch is required when the matter is released to another cleared contractor or OGA.
 - (3) Ash residue produced by burning must be examined and reduced by physical disturbance to ensure that the matter is completely destroyed and no ash residue matter remains to prevent the release of classified information or subsequent analysis.

- (4) Classified microforms must be destroyed by burning, chemical decomposition, disintegration, or other methods approved by the cognizant security authority.
 - (5) Classified ESM destruction must include examination to ensure that the media is no longer usable and that no classified information is present or recoverable. Classified ESM destruction must be completed in accordance with the DOE cyber security requirements.
 - d. Equipment. Classified matter must be destroyed by equipment that has been approved by the cognizant security authority and in accordance with specific manufacturer's instructions. The residue output must be inspected each time destruction is effected to ensure that established requirements have been met.
 - (1) Shredders.
 - (a) Crosscut shredders used for the destruction of classified paper matter and non-paper products, excluding microfilm, must produce residue with a particle size not exceeding 1 mm in width by 5 mm in length. (Note exception in following paragraph.)
 - (b) Crosscut shredders purchased prior to December 31, 2003, that produce residue with a particle sizes not exceeding 1/32 of an inch in width by 1/2 inch in length may continue to be used for the destruction of classified paper matter and non-paper products, excluding microfilm. However, these shredders must not be used once they cannot be repaired or restored to cut residue within the 1/32-inch width by 1/2-inch maximum particle dimensions.
 - (2) Pulping equipment must be equipped with security screens with perforations of 1/4 inch or smaller.
 - (3) Pulverizing equipment must be outfitted with security screens that meet the following specifications:
 - (a) Hammer mill perforations must not exceed 3/16 inch in diameter.
 - (b) Chopper and hybridized disintegrator perforations must not exceed 3/32 inch in diameter.
 - e. Witnesses.
 - (1) The destruction of classified matter must be ensured by an individual(s) who has/have appropriate security clearance for the classification level, category (if RD/FRD), and any applicable caveats of the matter to be destroyed.

- (2) The destruction of non-accountable classified matter may be accomplished by one individual; no witness is required.
- (3) The destruction of accountable classified matter must be witnessed by an appropriately cleared individual other than the person destroying the matter.

f. Destruction Records.

- (1) Accountable Matter. Destruction of accountable classified matter must be documented on DOE F 5635.9, *Record of Destruction*, or a form similar in content, which must be signed by both the individual destroying the matter and the witness.
- (2) Non-accountable Matter. Non-accountable matter does not require destruction receipts or certificates.

9. FOREIGN GOVERNMENT INFORMATION. The requirements in this paragraph are provided in addition to other protection and control measures in this Manual and are not applicable to NATO information. NATO information must be safeguarded in compliance with the U.S. Security Authority for NATO Instructions. Modifications to these requirements may be permitted by treaties, agreements, or other obligations with the prior written consent of the national security authority of the originating government.

- a. General. FGI must be safeguarded to provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When equivalent, standards may be less restrictive than the safeguarding standards that ordinarily apply to U.S. Confidential information, including allowing access to individuals with a need to know who have not otherwise been cleared for access to classified information.
- b. Classified Information Received from Foreign Governments. To ensure the protection of classified FGI in accordance with Executive Order 12958, as amended, the following requirements must be met.
 - (1) Handling. Classified documents received from foreign governments do not require portion marking. Such documents generated and marked entirely by a foreign government must be protected commensurate with the classification level the foreign government specified.
 - (2) Marking.
 - (a) A derivative classifier or classification officer must be contacted with any questions regarding the appropriate classification level for a FGI document.
 - (b) Documents generated by a foreign government in which U.S. information has been added must be reviewed for classification by

a derivative classifier or classification officer, marked, and protected accordingly.

- (c) If the original markings in the foreign government documents are readily recognizable as related to a U.S. classification requiring special protection and control, the documents do not require re-marking.
 - (d) If the foreign government marking is not readily recognizable as related to a U.S. classification, the foreign government document must be reviewed by a derivative classifier or classification officer, and an equivalent U.S. classification must be applied.
 - (e) If the fact that the information is FGI must be concealed, the document must be marked as if it were wholly of U.S. origin.
- (3) Confidential Foreign Government Information. Unless requested by the originating government, records are not required to be maintained for Confidential FGI.
 - (4) Secret Foreign Government Information. Secret FGI must be entered into accountability when required by treaties or international agreements.
 - (5) Top Secret Foreign Government Information. Top Secret FGI must comply with the requirements in Section A, Chapter II, Paragraph 5 above.
 - (6) Confidential Foreign Government Information–Modified Handling Authorized (C/FGI-MOD). If the foreign protection requirements are lower than the protection required for U.S. Confidential information, the following requirements must be met.
 - (a) Marking. If a document is determined to be C/FGI-MOD, in addition to other marking requirements above, the first page of the document must include:
 - 1 the derivative classifier marking, unless C/FGI-MOD can be determined by foreign markings, and
 - 2 the statement, “This document contains (*name of country*) (*classification level*) information to be treated as U.S. Confidential-Modified Handling Authorized.”
 - 3 the DOE F 470.9, *C/FGI-Mod Coversheet*, must be used.
 - (b) Access/Need to Know. Access to C/FGI–MOD matter does not require DOE security clearance. However, such documents must be provided only to those who have an established need to know and where access is required by official duties and who are citizens

from countries that have been authorized by the originating country.

- (c) Protection. C/FGI-MOD matter must be protected in the following manner.
 - 1 Protection in Use. Physical control must be maintained over any matter marked as containing C/FGI-MOD matter to prevent unauthorized access to the information.
 - 2 Protection in Storage. C/FGI-MOD matter must be stored to preclude unauthorized disclosure, at least equivalent to that stipulated by the foreign government.
- (d) Reproduction. Matter marked as containing C/FGI-MOD may be reproduced without permission of the originator to the minimum extent necessary to carry out official duties.
- (e) Destruction. When C/FGI-MOD matter is to be destroyed, it must be sufficiently destroyed to preclude recovery of any of the information it contained and in a manner approved for destruction of classified matter or as approved by the DOE cognizant security authority.
- (f) Transmission. C/FGI-MOD matter must be transmitted by means approved for transmitting classified matter unless this requirement is waived by the originating foreign government.

CHAPTER III. STORAGE REQUIREMENTS FOR CLASSIFIED MATTER

1. **STORAGE REQUIREMENTS.** The following physical security storage requirements apply to classified safeguards and security (S&S) interests.
 - a. **Restrictions on Secure Storage Repositories Used for Classified Matter.** Repositories used to store classified matter must not be used to store or contain other items that may be a substantial target for theft.
 - b. **Secure Storage Repository Requirements.** Security containers used for storing classified matter must conform to General Services Administration (GSA) standards and specifications. All GSA-approved security containers must be maintained within limited or higher security areas unless otherwise noted in this Manual. Vaults and vault-type rooms (VTRs) used for open storage of classified matter must meet the requirements of DOE M 470.4-2. (NOTE: The response times in this section do not apply to SAPs or SCI.)
 - (1) Classified matter that is not under the personal control of an individual with appropriate security clearance and need to know must be stored as described below.
 - (a) If inspections by Protective Force (PF) personnel are used as supplemental control, PF personnel must examine exposed surfaces of the secure storage repositories and steel filing cabinets for evidence of any forced entry to ensure that the security container or door is locked and the Standard Form (SF) 702 completely annotated.
 - (b) Areas and buildings must be protected from adversary access by application of GSA-approved locks and barriers. Requirements for these locks and barriers can be found in DOE M 470.4-2.
 - (2) Confidential matter must be stored in the same manner prescribed for Secret or Top Secret matter, but the supplemental controls are not required.
 - (3) Secret matter must be stored as described below or in any manner authorized for Top Secret matter.
 - (a) In a locked vault or in a locked GSA-approved security container within an LA or higher.
 - (b) In a locked VTR within an LA, Exclusion Area (EA), Protected Area (PA), or Material Access Area (MAA) equipped with intrusion detection system protection. PF personnel must respond within 30 minutes of alarm annunciation.

- (c) When located outside an LA, the locked vault or VTR must be under intrusion detection system protection. PF personnel must respond within 15 minutes of alarm annunciation.
- (d) In locked, steel filing cabinets that do not meet GSA requirements (containers purchased and approved for use before July 15, 1994, may continue to be used until October 1, 2012) and are equipped with three-position, dial-type, changeable combination locks. The cabinet must be in a locked area or building within the minimum of an LA. In addition, one of the following supplemental controls is required.
 - 1 Intrusion detection system protection that provides for response from PF personnel within 30 minutes of alarm annunciation.
 - 2 Inspection every 4 hours by PF or by cleared duty personnel when unattended.
- (4) Top Secret matter must be stored as described below.
 - (a) In a locked, GSA-approved security container with one of the following supplemental controls:
 - 1 under intrusion detection system protection and by PF personnel responding within 15 minutes of alarm annunciation; or
 - 2 inspections by PF personnel no less frequently than every 2 hours.
 - (b) In a locked vault or VTR within an LA, EA, PA, or MAA. The vault or VTR must be equipped with intrusion detection equipment, and PF personnel must respond within 15 minutes of alarm annunciation.
 - (c) In a locked vault or VTR within a property protection area (PPA) or outside of a security area, and it must be under intrusion detection system protection. PF personnel must respond within 5 minutes of alarm annunciation.
- (5) Nuclear weapon configurations, nuclear test and trainer devices, and nuclear-explosive-like assemblies without nuclear material must be stored in a vault or VTR located, at a minimum, within an LA. PF personnel must respond within 15 minutes of alarm annunciation. (The DOE physical security manual provides additional requirements.)

- c. Response Personnel. PF personnel, private security firms, or local law enforcement agency personnel must respond to intrusion detection system alarms as specified and documented in the Site Security Plan (see DOE M 470.4-1 Chg. 1 for additional information regarding S&S plans).
 - d. Alternative Storage Locations. Approved Federal Records Centers may be used to store classified information (see DOE M 470.4-1 Chg. 1).
 - e. Commingling Classified Matter.
 - (1) Classified and unclassified documents may be commingled. For example, Top Secret (TS), Confidential (C), and unclassified documents may be stored in the same file folder. Need-to-know considerations, however, might make it necessary to segregate documents (e.g., to avoid photographing Top Secret documents onto the same reel or microfiche as Secret (S) or Confidential documents). Good business practice suggests marking commingled unclassified documents as “Unclassified” when storing/filing with classified documents.
 - (2) Accountable Classified Removable Electronic Media must be separated from and not commingled with other classified information/media.
2. STORAGE—REPOSITORIES. When not in use, classified matter must be stored and locked in an approved secure storage repository unless otherwise noted in this Manual or DOE M 470.4-2. The following storage requirements apply to secure storage repositories that contain classified matter or other S&S interests.
- a. Security Containers.
 - (1) General. Secure storage repositories must not bear any external classification or other markings that would indicate the level of classified matter authorized to be stored within the container. For identification purposes, each security container must bear a uniquely assigned number on the exterior.
 - (2) Accountable Classified Removable Electronic Media (ACREM).
 - (a) All ACREM must be in a LA or higher security area when stored.
 - (b) Secure storage repositories that are used to store ACREM must be configured to provide limited access to ACREM by only the ACREM custodian(s) or alternate ACREM custodian(s).
 - (c) Keys and equivalent mechanisms allowing access to ACREM must be controlled to ensure only authorized ACREM custodians/alternates have access and the control system must be documented.

- (d) A seal must be affixed each time a security container being used to store ACREM that is located outside a vault or VTR is closed, and this action must be documented according to locally approved procedures to provide positive evidence of opening/tampering or access. Alternatively, if the security container is equipped with a XO-series lock prior to opening the container, the authorized opener must operate the lock to display the number of prior openings. The number indicated should correspond to that noted on the SF 702 from the previous opening. (If the number has advanced by one or more integers, the custodian must be alerted that the container had been opened with no record of such on the SF 702 and a security incident report must be filed if required by DOE M 470.4-1 Chg. 1.)

b. Documentation - SF 700, Security Container Information.

- (1) SF 700, Part 1 must be completed for each secure storage repository or other location approved for storing classified matter and include the names of all individuals who may be contacted if the container is found open and unattended. A record must be maintained of all individuals who have or may be granted access to the secure storage repository combination.
 - (a) The local implementation plan may dictate whether or not Block 8, *Serial No. of Lock*, must be left blank.
 - (b) SF 700, Part 1 must be affixed to the inside of the door of vaults and VTRs containing the combination lock. For security containers, it must be placed inside the locking drawer.
- (2) SF 700, Part 2a must be used to document the combination of the secure storage repository. It must be marked front and back with the highest level and most restrictive category (if RD or FRD) of information that may be stored within the repository and inserted in the accompanying envelope (part 2).
- (3) SF 700, part 2 (envelope) must be marked front and back with the highest level and most restrictive category (if RD/FRD) of information that may be stored within the secure storage repository. Once completed and sealed, it must be forwarded to central records for storage that prevents access by any individual who does not possess the same security clearance, any required formal access approval, and need to know. If the combination protects information requiring additional access approvals (e.g., Sigma 14, Sigma 15, North American Treaty Organization [NATO], Special Access Program [SAP] information, or Sensitive Compartmented Information [SCI]), the Part 2 must not be sent to central records unless all individuals at that location possess the same security clearance, any required formal access approval, and need to know.

- c. Combinations. Combinations to containers containing ACREM must be limited to the responsible ACREM primary and alternate ACREM custodian(s). When there are multiple shifts, the combination can be provided to the ACREM primary and alternate ACREM custodian(s) for each shift. A designated individual may be provided the combination only when the ACREM primary and all alternate ACREM custodian(s) are not available and access is required.
- (1) Changing Combinations. Combinations must be changed by an appropriately cleared and authorized individual as soon as practical after any of the following situations occur.
 - (a) Initial receipt of a GSA-approved security container or lock.
 - (b) When an individual who knows the combination—
 - 1 is reassigned, transferred, or terminated.
 - 2 has his/her security clearance downgraded to a level lower than the level of classified matter stored.
 - 3 has his/her security clearance administratively terminated or suspended.
 - (c) Maintenance is performed by a locksmith or safe technician.
 - (d) When the ACREM custodian(s) and/or alternate ACREM custodian(s) return after the combination has been provided to the designated individual.
 - (e) Compromise or suspected compromise of secure storage repository.
 - (f) Preparation for turning in a completely empty security container.
 - 1 The combination must be set to factory standard 50-25-50 before the container is turned in.
 - 2 When a security container is transferred from one organization to another, the custodian from the original organization must certify, in writing, that all classified matter has been removed before the transfer takes place.
 - (g) Combinations used to protect NATO material must be changed no less frequently than 12-month intervals.
- (2) Selection of Combination Settings. Combination numbers must be selected at random. Security containers with multiple locking drawers must contain a classified combination on each drawer.

(3) SF 701, Activity Security Check List.

- (a) The SF 701 provides a systematic means of checking end-of-day activities for a particular work area, allowing for employee accountability in the event that irregularities are discovered.
- (b) Use of SF 701 is optional except when local security and/or implementation plans require its use for detailed end-of-day security inspections.

(4) SF 702, Security Container Check Sheet.

- (a) The SF 702 must be used to record security checks each day a container may have been accessed by documenting the times and the initials of the person(s) who have opened, closed, or checked a particular container, room, vault, or VTR holding classified information. A sole custodian of a security container is not required to record each opening and closing of the container throughout the day. In such cases, the appropriate information must be recorded on the SF 702 the first time the container is opened that day. The container may be opened and closed as necessary without further record keeping. At the end of the day, information must be recorded indicating the final closing of the container for that day. When 24-hour operations are involved, another reasonable time period may be established to conduct end of the day/shift system checks.
- (b) The SF 702 must be used for any secure storage repository used to store ACREM, including locked drawers or file cabinets in vaults and VTRs and those that use XO-Series locks.
- (c) The SF 702 must be in a conspicuous location and affixed or in close proximity to each security container and/or the entrance to each vault or VTR.

3. NON-CONFORMING STORAGE. Classified matter must be stored under conditions designed to deter and detect unauthorized access to the matter, to include securing it in approved equipment or facilities whenever it is not under the direct control of an authorized person. Non-conforming storage may only be used for classified matter that cannot be protected by the established standards and requirements due to its size, nature, operational necessity, or other factors. In these exceptional cases, non-conforming storage that deters and detects unauthorized access to the classified matter may be used for storing classified matter.

Non-Conforming Storage must result in protection effectiveness equivalent to that provided to similar level(s) and categories of classified matter by standard configurations.

The methods, protection measures, and procedures must be documented and approved by the DOE cognizant security authority. Documentation must include the following:

- a. Explanation as to why exercising this option is necessary;
- b. Description of classified matter to be stored;
- c. Description of the means by which equivalent security is to be provided;
- d. An analysis demonstrating the equivalence of protection;
- e. A copy of the documentation must be maintained locally;
- f. Copies of the documentation must be forwarded to the cognizant Headquarters Departmental element; and
- g. Updates to this documentation as conditions change.

4. PERMANENT BURIAL.

- a. Burial is an option that may be approved by the DOE cognizant security authority for permanent placement of classified matter. In addition to meeting the requirements for non-conforming storage of classified matter, permanent burial documentation must also include:
 - (1) For active burial operations, description of the entire placement process, including protection of classified matter prior to final burial;
 - (2) Configuration of classified matter to be buried;
 - (3) Assurance that undisturbed burial is designed and will be sustained indefinitely for the buried classified matter;
 - (4) Explanation of current and future use of the burial location and all pertinent location characteristics (natural or engineered) that will limit or preclude access to the classified matter; and
 - (5) Updates to this documentation as conditions change.
- b. Classified matter that is accountable is considered to meet accountability requirements when it is permanently placed into an approved burial configuration.
- c. Inventory of previously accountable classified matter may be suspended indefinitely as long as there has been no access to the matter since it was buried.

SECTION B—OPERATIONS SECURITY

1. OBJECTIVES.

- a. To help ensure that Critical Program Information (CPI) is protected from inadvertent and unauthorized disclosure.
- b. To provide management with the information required for sound risk management decisions concerning the protection of sensitive information.
- c. To ensure that Operations Security (OPSEC) techniques and measures are used throughout the Department.

2. REQUIREMENTS.

- a. An OPSEC program(s) must be implemented, covering each program office, site, and facility to ensure the protection of CPI and to assist in ensuring the protection of classified matter. The OPSEC program, in addition to ensuring the compliance with the requirements of this Manual, must also include the following activities:
 - (1) Establish a point of contact with overall OPSEC responsibilities for each site, facility, and program office whose name and contact information will be provided to the Office of Health, Safety and Security.
 - (2) Ensure OPSEC point of contact participation in the development of local implementation training and/or briefings tailored to the job duties of the individual employees.
 - (3) Development and execution of a comprehensive OPSEC awareness program that includes regular briefings to ensure that personnel are aware of their responsibilities in support of the OPSEC program. These briefings provide local implementation of requirements and may be integrated into, or provided in conjunction with, required security briefings (e.g., new hires' initial briefings, comprehensive or annual refresher briefings).
 - (4) Participation in self-assessments to ensure the requirements to protect and control classified matter and CPI are being followed in all areas and that employees are aware of their responsibilities.
 - (5) Provision of information concerning deviations (e.g., variances, waivers, and exemptions) involving the OPSEC program to the Office of Health, Safety and Security and to the Associate Administrator for Defense Nuclear Security when involving National Nuclear Security Administration (NNSA) facilities, in a timely fashion, to include implementation and expiration of such actions. This may be accomplished through the Field or Site Office Manager as appropriate.
 - (6) Promulgation of new OPSEC requirements to all affected employees.

- (7) Interaction and coordination with Office of Health, Safety and Security on OPSEC National and Departmental requirements interpretation and local implementation activities. Interaction and coordination between NNSA facilities and the Office of Health, Safety and Security is through the Associate Administrator for Defense Nuclear Security.
- b. OPSEC plans must be developed for programs and operations and approved by the cognizant security authority.
- c. OPSEC plans must be reviewed and updated annually (at least every 12 months).
- d. CPI, formerly known as critical sensitive information, must be identified, including operational and programmatic data that would have a negative impact on national security and/or Departmental operations if unauthorized disclosure should occur. The CPI must be—
 - (1) prioritized according to the level of impact posed by an unauthorized disclosure. The CPI may be supported by a list of indicators that, when aggregated and analyzed, inappropriately reveal elements of the CPI.
 - (2) reviewed on a continuing basis. Results of the CPI reviews must be documented and maintained in program files.
- e. OPSEC assessments must be conducted at facilities having Category I special nuclear material (SNM) (or credible roll-up of Category II to a Category I quantity), Top Secret or Special Access Program (SAP) information within their boundaries. OPSEC assessments must be conducted at other facilities involved in creating, handling, storing, processing, transmitting, or destroying CPI as deemed necessary by the cognizant security authority.
 - (1) Either the programmatic or facility approach may be used to conduct OPSEC assessments. If the facility approach is used, all activities at the facility must be included in the assessment. If the programmatic approach is used, all activities within the program must be included in the assessment.
 - (2) When using the programmatic approach, the assessment team must ensure that CPI pertaining to Category I SNM (or credible roll-up of Category II to a Category I quantity), Top Secret matter, or SAPs are assessed. Schedule and priority for conducting assessments will be based on CPI, threat assessments, risk management principles, recommendations received from the local OPSEC program, and direction from Department of Energy (DOE) line management.
- f. OPSEC Reviews.

- (1) Reviews must be conducted to identify changing priorities in the local OPSEC program. OPSEC reviews are limited information-gathering activities to provide the data necessary to schedule and implement OPSEC actions. Results of OPSEC reviews must be documented.
 - (2) OPSEC reviews of sensitive activities and facilities must be conducted whenever the following criteria are met:
 - (a) New construction is planned for a facility that will process or store classified or sensitive information or matter.
 - (b) New sensitive activities are initiated or existing programs incur significant changes.
 - (c) A sensitive program or activity has not been the subject of an OPSEC assessment or OPSEC review for the preceding 2 years.
- g. Information to be posted to publicly available websites.
- (1) Before any information generated by or for the Federal Government (Government Information) is placed on a DOE, DOE contractor or sub-contractor website or is otherwise made available to the public, it must be reviewed to ensure that it does not contain classified information or CPI. Before DOE employees, DOE contractors, or sub-contractors post Government Information to a personal or non-DOE website, it must also be reviewed for the same concerns. The review process must include a multi-layer review to ensure suitability of the information for worldwide public release.
 - (2) Automated analysis tools should be used to assist in the review of information to determine if it is appropriate to release it to the public. Certain categories of unclassified information are generally recognized as unsuitable for public release. These include, but are not limited to, Official Use Only information, privacy information, protected Cooperative Research and Development Agreement information, Unclassified Controlled Nuclear Information, and Export Control Sensitive Subjects information. Due to the diversity of information that must be considered within DOE, a robust review and approval process must be conducted using the following evaluation factors for determining suitability for release of information to the public. Evaluation factors include:
 - (a) Sensitivity. If the information is released to the public, it must not reveal or identify sensitive information, activities or programs.
 - (b) Risk. Information that may be used by adversaries to the detriment of employees, the public, the Department or the nation must not be approved for release. This determination must be based on sound

risk management principles focused on preventing potential adverse consequences.

- (3) Heads of Departmental elements must document a program element position that identifies categories of information deemed inappropriate for public release and establishes review and approval procedures for all information being considered for release.
- (4) Local procedures must be established for conducting information reviews and acquiring approval according to direction from the Head of their respective Departmental element. These procedures must identify specific information and information categories considered unsuitable for release to the public.

SECTION C—SPECIAL ACCESS PROGRAMS

1. OBJECTIVES. To establish requirements for Special Access Programs (SAPs) authorized for use within the Department. (NOTE: Terms and activities such as Limited Access, Controlled Access, and Limited Distribution programs are not authorized.)
2. REQUIREMENTS.
 - a. All SAPs must be approved by the Secretary or Deputy Secretary, based upon the recommendation of the SAP Oversight Committee (SAPOC), which manages and oversees the development of SAP security policies and procedures outlined in DOE M 471.2-3B, *Special Access Program Policies, Responsibilities and Procedures*.
 - b. SAPs must be limited to acquisition, operations, support, and intelligence activities.
 - c. U.S. Department of Energy (DOE) and non-DOE (Work for Others) SAPs, with the exception of intelligence SAPs, must be registered manually (not in the Safeguards and Security Information Management System) through the established Facility Clearance process using DOE F 470.2, Facility Data Approval Record (FDAR) and DOE F 470.1, Contract Security Classification Specification, Department of Defense Form 254, or form similar in content. For additional information regarding the FDAR process, see DOE M 470.4-1 Chg. 1, *Safeguards and Security Program Planning and Management*. The FDAR and other forms must be classified in accordance with classification guidance. SAPs must be manually registered through the SAP Security Coordinator with the DOE SAP Security Program Manager. Intelligence SAPs must be manually registered with the Office of Intelligence and Counterintelligence (IN) in accordance with instructions provided by IN. Registration of all Intelligence SAPs, other than those housed in a sensitive compartmented information facility, will be coordinated between the DOE SAP Security Program Manager and the Intelligence Work for Others Coordinator.
 - d. SAP facilities, work areas and all activities must be surveyed according to DOE M 470.4-1 Chg. 1, *Safeguards and Security Program Planning and Management*, by the cognizant SAP Security Coordinator in coordination with the cognizant program office and/or sponsor. Intelligence SAPs must be surveyed by the Office of Intelligence and Counterintelligence in conjunction with the Sponsor. Independent oversight inspections must be performed for Departmental programs in accordance with DOE M 471.2-3B.
 - e. Protection program planning documents, including security plans and standard operating procedures, must comply with established SAP policies and program security manuals.

- f. Any possible or probable loss, compromise, or unauthorized disclosure of SAP information must be reported to the appropriate Government Program Manager, Government Program Security Officer, DOE SAP Security Program Manager (or Cognizant SAP Security Coordinator) and the SAPOC's Executive Secretary in accordance with established procedures. (DOE M 470.4-1 Chg. 1, *Safeguards and Security Program Planning and Management*, Section N, contains additional requirements.)

SECTION D—TECHNICAL SURVEILLANCE COUNTERMEASURES

This Section is Official Use Only

Please contact the DOE Office of Health, Safety and Security
at (301) 903-0292 to request a copy of Section D

ATTACHMENT 1

INFORMATION SECURITY CONTRACTOR REQUIREMENTS DOCUMENT

This Contractor Requirements Document (CRD) establishes the security requirements for the protection and control of matter required to be classified or controlled by statutes, regulations, or U.S. Department of Energy (DOE) directives. DOE M 470.4-7, *Safeguards and Security Program References*, contains definitions, acronyms and references that apply to the Safeguards and Security Program.

All information security programs, practices, and procedures developed by the contractor must be consistent with and incorporate the requirements of this CRD along with the requirements that govern information security (See General Requirements - Paragraph 2, below, in this CRD, and the CRD to DOE M 470.4-7, *Safeguards and Security Program References*, Section B, under Information Security.). The information security program requirements discussed in this CRD include Classified Matter Protection and Control (CMPC), security of classified Foreign Government Information, Operations Security (OPSEC), security of Special Access Programs (SAPs), and Technical Surveillance Countermeasures (TSCM).

A violation of the provisions of this CRD relating to the safeguarding or security of Restricted Data or other classified information may result in a civil penalty pursuant to subsection a. of section 234B of the Atomic Energy Act of 1954 (42 U.S.C. 2282b.). The procedures for the assessment of civil penalties are set forth in Title 10, *Code of Federal Regulations* (CFR), Part 824, "Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations."

This CRD consists of four sections that provide direction for CMPC, OPSEC, security of SAP, and TSCM. Section A, CMPC, has three chapters. Chapter I provides the CMPC planning requirements. Chapter II provides CMPC requirements. Chapter III provides storage requirements for classified matter. Section B provides requirements for OPSEC. Section C presents requirements for SAPs. Section D provides requirements for TSCM.

GENERAL REQUIREMENTS.

1. Contractors are responsible for flowing down the requirements of the CRD to subcontractors at any tier to the extent necessary to ensure compliance with the requirements. In doing so, contractors must not unnecessarily or imprudently flow down requirements to subcontracts. That is, contractors must both ensure that they and their subcontractors comply with the requirements of this CRD and only incur costs that would be incurred by a prudent person in the conduct of competitive business.
2. The following references include additional information security requirements:
 - a. 18 U.S.C. 798, Disclosure of Classified Information.
 - b. 42 U.S.C., Chapter 23. [Atomic Energy Act of 1954 (AEA), as amended].
 - c. 50 U.S.C. 2426, Congressional Oversight of Special Access Programs.

- d. Title 10, Code of Federal Regulations, Energy, Parts 725, 824, 1016, 1017, 1044, 1045, and 1046.
- e. Title 32 Code of Federal Regulations, Chapter XIX, Central Intelligence Agency.
- f. Title 32 Code of Federal Regulations, Chapter XX, Information Security Oversight Office, National Archives and Records Administration.
- g. Title 48 Code of Federal Regulations, Chapter 9, Department of Energy (DEAR 952.204).
- h. Executive Order 12333, United States Intelligence Activities.
 - (1) Amended by: EO 13284, Amendment of Executive Orders, and Other Actions, in Connection With the Establishment of the Department of Homeland Security.
 - (2) Amended by: EO 13355, Strengthened Management of the Intelligence Community.
- i. Executive Order 12829, National Industrial Security Program.
- j. Amended by E.O.12885, Amendment to Executive Order No. 12829.
- k. Executive Order 12958, Classified National Security Information.
 - (1) Amended by E.O. 12972, Amendment to Executive Order No. 12958.
 - (2) Amended by E.O. 13142, Amendment to Executive Order 12958 Classified National Security Information.
 - (3) Amended by E.O. 13292, Further Amendment to Executive Order 12958, as Amended, Classified National Security Information.
- l. Executive Order 12968, Access to Classified Information.
- m. Executive Order 13462, President's Intelligence Advisory Board and Intelligence Oversight Board.
- n. National Security Decision Directive 19, Protection of Classified National Security Council and Intelligence Information.
- o. National Security Decision Directive 84, Safeguarding National Security Information.
- p. National Security Decision Directive 298, National Operations Security Program.

- q. NDP-1, National Policies and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organization.
- r. National Industrial Security Program Operating Manual.
- s. National Industrial Security Program Operating Manual Operating Manual Supplement.
- t. NAVSEAINST C5511.32B, Safeguarding of Naval Nuclear Propulsion Information (NNPI) (U).
- u. Security Policy Board Issuance 4-97, National Policy on Reciprocity of Use and Inspection of Facilities.
- v. Security Policy Board SPB Issuance 5-97, Guidelines for the Implementation and Oversight of the Policy on Reciprocity of Use and Inspection of Facilities.
- w. DOE O 200.1, *Information Management Program*, dated 9-30-96.
- x. DOE M 200.1-1 Chapter 9, *Public Key Cryptography and Key Management*, dated 2-15-00.
- y. DOE P 205.1, *Departmental Cyber Security Management Policy*, dated 5-8-01.
- z. DOE M 205.1-3, *Telecommunications Security Manual*, dated 4-17-06.
- aa. DOE M 205.1-4, *National Security System Manual*, dated 3-8-07.
- bb. DOE M 205.1-5, *Cyber Security Process Requirements Manual*, dated 8-12-08.
- cc. DOE O 205.1A, *Department of Energy Cyber Security Management*, dated 12-4-06.
- dd. DOE O 241.1A Chg 1, *Scientific and Technical Information Management*, dated 10-14-03.
- ee. DOE M 452.4-1A, *Protection of Use Control Vulnerabilities and Designs*, dated 3-11-04.
- ff. DOE P 470.1, *Integrated Safeguards and Security Management (ISSM) Policy*, dated 5-8-01.
- gg. DOE O 470.3B, *Graded Security Protection (GSP) Policy*, dated 8-12-08.
- hh. DOE M 470.4-1 Chg 1, *Safeguards and Security Program Planning and Management*, dated 8-26-05.
- ii. DOE G 470.4-1, *Asset Protection Analysis Guide*, dated 8-21-08.

- jj. DOE M 470.4-2 Chg 1, *Physical Protection*, dated 8-26-05.
- kk. DOE M 470.4-3 Chg 1, *Protective Force*, dated 8-26-05.
- ll. DOE M 470.4-5, *Personnel Security*, dated 8-26-05.
- mm. DOE M 470.4-6 Chg 1, *Nuclear Material Control and Accountability*, dated 8-26-05.
- nn. DOE M 470.4-7, *Safeguards and Security Program References*, dated 8-26-05.
- oo. DOE O 470.4A, *Safeguards and Security Program*, dated 5-25-07.
- pp. DOE M 471.1-1 Chg 1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual*, dated 10-23-00.
- qq. DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*, dated 6-30-00.
- rr. DOE M 471.2-3B, *Special Access Program Policies, Responsibilities, and Procedures*, dated 10-29-07.
- ss. DOE O 471.3, *Identifying and Protecting Official Use Only Information*, dated 4-9-03.
- tt. DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, dated 4-9-03.
- uu. DOE G 471.3-1, *Guide to Identifying Official Use Only Information*, dated 4-9-03.
- vv. DOE O 475.1, *Counterintelligence Program*, dated 12-10-04.
- ww. DOE M 475.1-1 B, *Manual for Identifying Classified Information*, dated 8-28-07.
- xx. DOE O 475.2, *Identifying Classified Information*, dated 8-28-07.
- yy. DOE O 5610.2 Chg 1, *Control of Weapon Data*, dated 9-2-86.
- zz. DOE O 5639.8A, *Security of Foreign Intelligence Information and Sensitive*, dated 7-23-93.
- aaa. Compartmented Information Facilities.
- bbb. DOE O 5670.1A, *Management and Control of Foreign Intelligence*, dated 1-15-92.
- ccc. DOE Sensitive Compartmented Information Facility Procedural Guide.

3. Deviations from national regulations, including the Code of Federal Regulations, and national-level policies are subject to the deviation process of the governing document rather than the DOE deviation process. This directive conveys no authority to deviate from law. Requests for deviations from requirements specific to DOE, including this Manual, must be processed in accordance with the provisions of DOE M 470.4-1 Chg. 1, *Safeguards and Security Program Planning and Management*.
4. Requirements that cannot be implemented within 6 months of the addition of this CRD to the contract or with existing resources must be documented by the contractor's cognizant security authority and submitted to the Field or Site Office Manager for submission to the relevant program officers; the Under Secretary for Energy, the Under Secretary for Science, or the Under Secretary for Nuclear Security/Administrator, NNSA; and the Office of Health, Safety and Security. The documentation must include timelines and resources needed to fully implement this CRD. Requests for deviations from requirements specific to this CRD must be processed in accordance with the CRD deviation section of DOE M 470.4-1 Chg. 1, *Safeguards and Security Program Planning and Management*.

TABLE OF CONTENTS

ATTACHMENT 1 INFORMATION SECURITY CONTRACTOR REQUIREMENTS DOCUMENT.....	I
GENERAL REQUIREMENTS.....	I
SECTION A - CLASSIFIED MATTER PROTECTION AND CONTROL.....	A-1
1. OBJECTIVES	A-1
2. REQUIREMENTS.....	A-1
CHAPTER I . PROTECTION AND CONTROL PLANNING	I-1
1. CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) PROGRAM IMPLEMENTATION	I-1
2. PROTECTION STRATEGIES & PLANNING	I-1
3. DISCLOSURE AND RELEASE OF CLASSIFIED MATTER	I-1
4. TRAINING	I-4
CHAPTER II . CLASSIFIED MATTER PROTECTION AND CONTROL REQUIREMENTS	II-1
1. GENERAL.....	II-1
2. CLASSIFIED MATTER IN USE.....	II-2
3. MARKING	II-3
4. MARKING MATERIAL.....	II-8
5. CONTROL SYSTEMS AND ACCOUNTABILITY.....	II-9
6. REPRODUCTION.....	II-14
7. RECEIVING AND TRANSMITTING CLASSIFIED MATTER	II-15
8. DESTRUCTION.....	II-24
9. FOREIGN GOVERNMENT INFORMATION	II-26
CHAPTER III . STORAGE REQUIREMENTS FOR CLASSIFIED MATTER.....	III-1
1. STORAGE REQUIREMENTS	III-1
2. STORAGE—REPOSITORIES	III-3
3. NON-CONFORMING STORAGE	III-6
4. PERMANENT BURIAL	III-7
SECTION B - OPERATIONS SECURITY	B-1
1. OBJECTIVES	B-1
2. REQUIREMENTS.....	B-1

SECTION C - SPECIAL ACCESS PROGRAMS.....	C-1
1. OBJECTIVES	C-1
2. REQUIREMENTS.....	C-1
SECTION D - TECHNICAL SURVEILLANCE COUNTERMEASURES	D-1

SECTION A - CLASSIFIED MATTER PROTECTION AND CONTROL

1. OBJECTIVES.

- a. To protect and control classified matter that is generated, received, transmitted, used, stored, reproduced, permanently buried according to the requirements of this CRD, or to be destroyed.
- b. To establish the requirements for an audit trail for all accountable classified matter.
- c. To establish required controls based on classification level (Top Secret, Secret, or Confidential); category (Restricted Data [RD], Formerly Restricted Data [FRD]), or National Security Information [NSI]); and special handling instructions or caveats.

2. REQUIREMENTS.

- a. Classified matter that is generated, received, transmitted, used, stored, reproduced, permanently placed (buried according to the requirements of this CRD), or destroyed must be protected and controlled commensurate with classification level, category (if RD/FRD), and caveats (if applicable). All pertinent attributes must be used to determine the degree of protection and control required to prevent unauthorized access to classified matter.
- b. Classified information must only be processed on information systems that have received authority to operate according to DOE Office of the Chief Information Officer directives that establish requirements for national security systems.
- c. Local processes and procedures to implement the national and departmental requirements must be established for the protection and control of classified matter. These processes and procedures must include audit trails for all accountable classified matter.
- d. Buildings and rooms containing classified matter must be configured with security measures, which prevent unauthorized persons from gaining access to classified matter; specifically, security measures that prevent unauthorized physical, visual, and aural access.
- e. Secret matter that cannot be processed, handled, and/or stored within an LA or higher must be maintained in an accountability system as described in Chapter II of this CRD.
- f. Need-to-know controls, appropriate physical security, and access control measures must be applied to each area or building within a security area where classified matter is processed, handled or stored to detect unauthorized access.

- g. Retention Requirements. All records associated with the protection and control of classified matter must be maintained in accordance with the most current National Archives Records Administration General Records Schedule 18, Security and Protective Services Record.
- h. Reporting Requirements. Incident reporting requirements and instructions are contained in the CRD to DOE M 470.4-1 Chg. 1.

CHAPTER I. PROTECTION AND CONTROL PLANNING

1. CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) PROGRAM IMPLEMENTATION.

- a. To ensure the protection and control of classified information and matter, a CMPC program must be implemented to cover each Departmental element, site and/or facility and must be tailored to achieve the protection levels that adequately address specific site characteristics and requirements, current technology, ongoing programs, and operational needs.
- b. The CMPC Program, in addition to ensuring compliance with the requirements of this CRD, must also include the following activities:
 - (1) Establishment of a point of contact with overall CMPC responsibilities for each site and/or facility.
 - (2) CMPC point(s) of contact must ensure the content of local CMPC training and/or briefings and awareness is commensurate with personnel responsibilities in support of the CMPC program.
 - (3) Promulgation of CMPC requirements to all affected employees.

2. PROTECTION STRATEGIES & PLANNING.

- a. Strategies for the protection and control of classified matter must incorporate the applicable requirements established in this CRD.
- b. The level of protection and resources expended on CMPC program must be commensurate with their effect deterring or detecting compromise of or unauthorized access to classified matter. Protection measures should provide a graded approach, identifying each layer of protection between the adversary and the asset.
- c. Safeguards and Security Plans. The details of site protection measures for classified matter must be described in applicable Site Security Plans (SSP) (see DOE M 470.4-1 Chg. 1).

3. DISCLOSURE AND RELEASE OF CLASSIFIED MATTER.

- a. Disclosure of Classified Information. In the event an emergency situation necessitates the intentional disclosure of classified information to individuals who are not otherwise eligible for access, the following actions must be taken if such an intentional release is required:
 - (1) Notification of Release. The following individuals must be notified through line management as soon as possible of any emergency release of

classified information to an individual or individuals who are otherwise not eligible for such access.

- (a) For RD or FRD: the Chief, Health, Safety and Security Officer; the head of the Departmental element; and the Associate Administrator for Defense Nuclear Security.
- (b) For National Security Information (NSI): the appropriate DOE line management or DOE cognizant security authority.

(2) Protection Measures.

- (a) The amount of classified information disclosed and the number of individuals to whom such information is disclosed must be limited to the absolute minimum to achieve the intended purpose.
- (b) If the information must be transmitted, it must be transmitted via approved channels if possible, or using the most secure and expeditious method if approved channels are not an option.
- (c) A description of what specific information is classified and protection requirements for the information must be provided to the recipient.
- (d) A briefing must be provided to the recipient covering requirements for not disclosing the information, and a nondisclosure agreement must be signed by the recipient.

b. Release of Classified Information to Foreign Governments. A contractor must not release any classified information to foreign governments without the express written approval of DOE. To ensure the protection of classified information, the following must be met:

- (1) National Disclosure Policy Committee (NDPC). The multi-agency NDPC, of which DOE is a "Special Member," governs the export of classified U.S. military information and material to foreign governments as provided for in international agreements. To ensure uniform application of safeguards, these agreements include arrangements for the appropriate safeguarding of information and material provided to DOE. Access to classified information and material must be granted in accordance with established international agreements.

DOE has agreed to inform the NDPC of international agreements involving the sharing of all classified information, including those made under the auspices of the Atomic Energy Act. This notification must include the provisions of security agreements that apply to the shared information. DOE is also required to coordinate with the Joint Atomic

Information Exchange Group (JAIEG) before disclosing atomic information (which includes RD and FRD).

- (2) Requests for Release of Classified Information to Foreign Governments or Their Representatives. Contractors must submit requests for release of U.S. classified information to any foreign government or their representatives to the Departmental element with cognizance over the information. The contractor must assist the cognizant Departmental element with the development of the release justification (See Section A, Chapter 1, paragraph 3.b.(4)(a) in DOE M 470.4-4A, Information Security). The Departmental element will then initiate review and final approval actions after determining that the required information submitted by the contractor is complete and accurate.
- (3) Required Approval. Contractors must not release any U.S. classified information to foreign governments without the prior written approval of DOE, or in the case of restricted data/formerly restricted data, the contractor must also receive the written approval of the JAIEG. The JAIEG approval must be acquired through the NNSA Deputy Administrator for Defense Programs.
- (4) Protection of Foreign Government Information Containing Unclassified United States Information. Documents containing U.S. unclassified information and FGI must be protected at the most restrictive level contained within the document.
- (5) Transmittal of Classified Information and Classified Matter. All transmittals that involve classified information or classified matter must be made by DOE unless the contractor has prior written authorization. If the transfer involves classified information or classified matter produced by or received from another Government agency, the cognizant Departmental element must obtain approval from the agency before transmission.
- (6) Returning Foreign Government Information Documents. If it is necessary to return the enhanced FGI (e.g., additional U.S. information added) to the originating government or international organization, it must be handled in accordance with paragraph 3.b above.
- (7) Preparation and Method of Transmission. Normally, documents intended for foreign governments must be forwarded to the receiving country's embassy in the United States. The method of transmission of classified mail to foreign countries must be approved by the Office Health, Safety and Security.
- (8) Transmittal Documentation. Contractors must submit a request and receive approval for physical transfers or oral disclosures, made or contemplated, from the cognizant Departmental element.

- (9) Oral Disclosure Records. A memorandum must be prepared for all actual and/or contemplated oral disclosures and provided to the DOE CSA. That memorandum must be contained in the oral disclosure records of the cognizant Departmental element and maintained by the cognizant program office.
- 4. TRAINING. All CMPC-related training/briefing regarding the local implementation of this CRD must be formally documented. It must also be approved by the cognizant security authority (e.g., frequency, content). (Specific training requirements, in addition to those stated in this CRD, are included in DOE M 470.4-1 Chg. 1.).
 - a. Each individual identified as a CMPC point-of-contact, according to Section A, Chapter 1, paragraph 1.b.(1) must receive initial training within one (1) year of appointment or as soon as training is available through the National Training Center (NTC). Other personnel may also receive the NTC-developed training.
 - b. All personnel with security clearances whose classified matter responsibilities include access (potential or actual), originating, handling, using, storing, accounting for, reproducing, transmitting (including hand-carrying), destroying, and/or emergency reporting must receive CMPC training and/or briefings commensurate with these responsibilities prior to receiving access to classified matter and receive refresher training and/or briefings to ensure continued reinforcement of requirements. This training and/or briefing must be tailored to the assigned duties and responsibilities of the persons receiving the training and/or briefing.
 - c. Personnel with security clearances whose job responsibilities do not meet the conditions specified in paragraph (b) above (e.g., personnel employed in maintenance, janitorial, food service, and other such activities) must receive training and/or briefings and be able to identify unprotected classified matter (e.g., by classified cover sheets and classification markings) and know the associated reporting requirements.

CHAPTER II. CLASSIFIED MATTER PROTECTION AND CONTROL REQUIREMENTS

1. GENERAL. Protection and control requirements include the following:
 - a. Prior to classification review, matter that may be classified must be protected at the highest potential classification level and category. The originator is responsible for obtaining a classification review by a derivative or original classifier if there are any questions regarding the classification of any draft document or working paper.
 - b. When information is prepared on classified information systems, the hard-copy output (which includes paper, microfiche, film, and other media) must be marked either:
 - (1) with the appropriate markings for the classification of the information as determined by a derivative classifier according to a classification review of the actual output,
 - (2) as a working paper or electronic medium to the accreditation level and category of the information system (see Chapter II, paragraph 3.p. for additional requirements that apply, regarding draft and working papers) or
 - (3) according to the marking requirements for the appropriate classification of information that has been generated by a program verified and formally approved by the Designated Approving Authority (DAA) to produce consistent results. The following factors must be satisfied when exercising this option:
 - (a) The output that will be produced must be fully defined and documented. The DAA must formally approve this documentation and must ensure that any subsequent output marked according to this option completely matches the planned and actual output for which the Classification Officer determined the classification level (and category if Restricted Data [RD] or Formerly Restricted Data [FRD]),
 - (b) The Classification Officer must review the fully defined output and must determine the correct classification level (and category if RD or FRD) for the information contained in the output, and
 - (c) All output must be marked with the correct classification level (and category if RD or FRD) as determined by the Classification Officer.
 - c. When matter must be sent outside the office of origin for a classification review and determination, it must be marked "DRAFT—Not Reviewed for

Classification.” To preclude marking every page of a document being transmitted for classification review, it should have a “Document Undergoing Classification Review” cover sheet that is marked with the highest level and most restrictive category of information the originator believes is contained in the document.

- d. Access to classified matter in an emergency involving an imminent threat (explosion, fire, etc.) to life or defense of the homeland may be provided to individuals who are not otherwise routinely eligible for access to classified matter. If an emergency is life-threatening, the health and safety of individuals takes precedence over the need to protect classified matter from disclosure. Examples of such releases include providing law enforcement personnel with classified information concerning an improvised nuclear device found in a public place, sharing a classified DOE evaluation of the viability of a nuclear threat message with local emergency response personnel, or providing an attending physician with classified details about nuclear materials at a site to assist in the emergency treatment of a patient.
 - (1) Protecting Classified Matter in Emergency Situations. DOE Cognizant Security Authority-approved procedures must be developed. These procedures must describe the actions (i.e., notifications, alternative storage, and protection methods) to be taken at the time of the emergency.
 - (a) Every attempt must be made to minimize access by uncleared emergency response personnel to only those areas directly affected by the emergency situation.
 - (b) All unsecured classified matter must be accounted for following the emergency.
 - (c) Secure storage repositories must be inspected on return to the facility to ensure they have not been compromised.
 - (2) Emergency Evacuation Drills/Tests. Emergency evacuation drill/test procedures must include protection requirements and Cognizant Security Authority (CSA)-approved procedures for protecting all classified matter from unauthorized access.
 - (3) Reporting Requirements. Report in accordance with incident reporting instructions contained in DOE M 470.4-1 Chg. 1.
2. CLASSIFIED MATTER IN USE. Classified matter in use must be constantly attended by or under the control of a person possessing the proper security clearance and need to know.
3. MARKING. All classified matter, regardless of level and category, must be marked to ensure information is appropriately protected to prevent inadvertent disclosure. Classified matter must be reviewed and brought up to current marking standards whenever it is

released by the current holder (“current holder” may be defined as an individual, specific office, or ad-hoc working group [AHWG]) or removed from archival storage. Marking requirements for foreign government information (FGI) are found in 9.b below. Marking examples can be found in the *DOE Marking Handbook* (see http://www.pnl.gov/isrc/pdf/doe_marking_handbook_2006.pdf).

a. General.

- (1) Requirements. Classified matter, regardless of date or agency of origin, must be marked to indicate at least the classification level and category (if RD or FRD).
 - (a) Classified NSI documents that were created after April 1, 1996, and that lack appropriate current markings including declassification on a date or event, classification basis, or classifier’s name, must be reviewed by a derivative classifier to ensure the classification level and category are still correct and then re-marked to bring them up to current marking requirements.
 - (b) Classified matter retained for litigation or for official archival purposes, including classified matter transferred during site closure, need not be brought up to current marking standards.
 - (c) DOE M 475.1-1B, *Identifying Classified Information*, provides requirements for reviewing and marking documents with obsolete markings.
- (2) Markings. All classification markings must be distinguishable from the document text. The overall classification level (i.e., Top Secret, Secret, or Confidential) of a document must be marked on the top and bottom of the cover page (if any), the title page (if any), the first page of text, and the outside of the back cover or last page of text. The classification level and category (if RD or FRD) must be clearly marked on all other (non-document) classified matter if possible. Otherwise, alternative marking methods must be used to identify the overall classification level and category (if RD or FRD). When marking the level or category is not practical, written notification must be furnished to all recipients. The originator is responsible for ensuring that classified matter is marked in accordance with this CRD. DOE M 475.1-1B contains additional marking requirements beyond the requirements contained in this CRD.

All interior pages of documents must be marked top and bottom with either:

- (a) The overall classification level and category (if RD or FRD) for the entire document, or

- (b) The highest classification level and category (if RD or FRD) of all information on that page; or with appropriate unclassified marking (e.g., Unclassified, OOU, UNCI) if there is no classified information on that page.
 - (3) Unique Identification Numbers. Classified matter required to be in accountability, as defined in Section A, Chapter II, paragraph 5, must have a unique identification number.
- b. Originating Organization and Date. The name and address of the organization responsible for preparing the document and the date of preparation must appear on the first page of all classified documents.
- c. Classification Categories. The three classification categories are RD, FRD, and NSI. Classified matter containing only NSI is *not* marked with a NSI admonishment.
 - (1) If the document contains RD or FRD information, the appropriate admonishment information must be marked on the first page of the document, whether cover page, title page, or first page of text and appear in the lower left corner.
 - (2) RD or FRD documents generated prior to July 9, 1998, are not required to be re-marked to indicate the category on each page containing RD or FRD information unless they are sent outside the office of origin or holder for other than archiving purposes.
- d. Mixed Levels and Categories. When classified matter contains a mix of information at various levels and categories that causes the document to be marked at an overall level and category higher than the protection level required for any of the individual portions, a marking matrix may be used in addition to other required markings. This would allow an individual with a lower access level, such as an "L" cleared employee, to be given access to a document that they might not otherwise have been authorized access to if the document was only marked at the highest overall classification level and category. (For example, a document that contains Confidential RD and Secret NSI would be required to be marked as Secret RD, the highest level and most restrictive category. None of the information in the document is Secret RD). However, this may not be interpreted to authorize any individual to gain access to information that exceeds their security clearance, formal access approvals, and need to know.

If the marking matrix is used, the following marking, in addition to other required markings, must be placed on the first page of text. The marking should appear on the lower right corner near the classifier information marking. If the derivative classifier places this marking on the document at the time of the classification decision, there is no need to indicate the name and title of the derivative classifier on the mixed level and category marking.

This document contains:

Restricted Data at the (e.g., *Confidential*) level.
Formerly Restricted Data at the (e.g., *Secret*) level.
National Security Information at the (e.g., *Secret*) level.

Classified by: *Name and Title*

- e. Components. When components of a document are to be issued or used separately, each major component must be reviewed and marked as a separate document. Components include annexes or appendixes, attachments, and major sections of a report. If an entire major component is unclassified, "Unclassified" must be marked at the top and bottom of the first page and a statement included (e.g., "All portions of this [annex, appendix, etc.] are Unclassified"). When this method of marking is used, no further markings are required on the unclassified component. Documents transmitted with a letter of transmittal are discussed in paragraph 3.o. below, Transmittal Documents.
- f. Unclassified Matter.
 - (1) Unclassified matter need not be marked unless it is essential to convey one of the following conditions:
 - (a) The matter has been reviewed for classification and does not contain classified information; or
 - (b) The matter has been properly declassified.
 - (2) If unclassified matter is marked, the Unclassified marking must be placed on the top and bottom of the front cover (if any), title page (if any), and first page of text.
- g. Portion Marking.
 - (1) NSI documents dated after April 1, 1997, must be portion marked.
 - (2) Documents containing RD or FRD should not be portion marked; however, if portion-marked, markings must be consistent with this Chapter.
 - (3) Portion markings must include any applicable caveats. Each section, part, paragraph, graphic, figure, subject/title, or similar portion of any such document must be accurately marked to show:
 - (a) the classification level, category (if RD or FRD), and caveat (e.g., S/RD, S/FRD, C/RD, C/FRD, S, TS, S/NOFORN, etc.); or
 - (b) that it is unclassified [e.g., (UCNI), (OUO), or (U)].

- (4) Page changes to NSI documents dated after April 1, 1997, must be portion marked. Additionally, any NSI document that becomes active (i.e., when it is released by the current holder - which may be defined as an individual, specific office, or AHWG - or removed from archival storage) must be portion marked with the appropriate classification level, caveat, or unclassified.
- (5) Portions of U.S. documents containing Foreign Government Information (FGI) must be marked to reflect the foreign country of origin and appropriate classification level (e.g., U.K.-C, indicating United Kingdom-Confidential). FGI must be indicated in lieu of the country of origin if the foreign government indicates it does not want to be identified.
- (6) Classification by Association or Compilation. DOE M 475.1-1B contains portion marking and other requirements for classified matter determined to be classified by association or compilation.
- h. Subjects and Titles. Titles must be marked with the appropriate classification (level; category if RD or FRD; and other applicable caveats) or control symbol or "U" if unclassified and placed immediately after the item.
- i. Classifier Markings. Classifier marking requirements can be found in DOE M 475.1-1B.
- j. Caveats and Special Control Markings. Caveats and special control markings are placed on documents to identify special handling or dissemination requirements or to assist in describing the type of information involved or who distributed or originated the information. Caveats and special control markings and any related admonishment statements or notices should be placed above the category admonishment statement, if any, on the lower left corner of the first page (cover page, if any; title page, if any; or first page of text) and in portion markings, when required.
- k. Re-marking Upgraded, Downgraded, and Declassified Matter. Requirements for marking upgraded, downgraded, or declassified matter are contained in DOE M 475.1-1B.
- l. Re-marking Automatically Declassified Matter. Matter marked for automatic declassification must not be re-marked unless it has been reviewed and determined by an Authorized Derivative Declassifier not to contain classified information (see DOE M 475.1-1B).
- m. Classified Matter Not Automatically Declassified. For requirements see DOE M 475.1-1B.

- n. File Folders and Other Containers. File folders and other items containing classified matter, when removed from secure storage repositories, must be conspicuously marked to indicate the highest classification level of their contents.
- o. Transmittal Documents. The first page of a transmittal document must be marked with the highest level and most restrictive category (if RD or FRD) of classified information being transmitted and with an appropriate notation to indicate its classification when the enclosures are removed.
- p. Working Papers and Drafts. Classified working papers and drafts are considered to be interim production stages toward the generation of a final document.
 - (1) Hard copies of working papers and drafts must contain the following markings:
 - (a) the date created;
 - (b) the highest potential overall classification level of the draft or working paper at the top and bottom of the outside of the cover page (if any), on the title page (if any), on the first page of text, and on the outside of the back cover or last page. Each interior page of a classified document must be marked at the top and bottom with the highest potential classification level of that page (including unclassified) or the overall classification of the document;
 - (c) the overall category (if RD or FRD) of the draft or working paper must be marked on the cover page (if any), title page (if any), or the first page of text. The category marking is not required on draft and working paper interior pages that contain RD or FRD information;
 - (d) the annotation “Working Paper” or “Draft” must be marked on the first page of text; and
 - (e) any applicable caveats or special markings must be annotated on the cover page (if any), title page (if any), or the first page of text.
 - (2) Markings prescribed for a finished document must be applied when a draft or working paper meets any of the following requirements:
 - (a) released by the originator outside the activity, office, or AHWG
 - (b) Top Secret retained for more than 30 days from the date of origin;
 - (c) Secret or Confidential retained for more than 180 days from the date of origin; or
 - (d) it will no longer be revised.

- (3) Classified documents that are updated on a frequent basis, commonly referred to as “living” documents (e.g., documents that are part of an ongoing experiment or study) may be considered as originating on each date they are changed. Local procedures must document specific techniques to demonstrate that working papers and drafts are “living” documents (e.g., a sheet attached to the front of the document that gives the number of pages or date of the last change is an example of such a technique).
 - (4) See Section A, Chapter II, Paragraph 1.c. for requirements for documents undergoing classification review.
- q. Redacted Documents. Methods used to strike out classified information before release to persons not authorized access to the deleted information must completely obliterate the classified text, figures, etc., to prevent any form of recovery that might compromise the information. DOE M 475.1-1B contains additional redaction requirements.
- r. Other Government Agency (OGA) Not Conforming to DOE Requirements. As a rule, documents received from OGAs and foreign governments that have not been marked to conform to DOE requirements do not need to be re-marked. However, all documents received must clearly indicate a classification level and category (if RD or FRD). The sender must be contacted to resolve any marking questions.
- s. Cover Sheets. Cover sheets must be applied to all classified documents when they are removed from a secure storage repository. (Reference: Standard Forms 703, 704, and 705)
- 4. MARKING MATERIAL.
 - a. Requirements. The classification level and category (if RD or FRD) must be conspicuously marked on all classified material. When marking is not practical, written notification of the markings must be furnished to recipients.
 - b. Caution. Before initiating any new marking policies, it is necessary to coordinate with the production engineers. War reserve and configuration control requirements mandate strict control over what is done to specific materials—markings cannot violate these rules. Any alternative markings under consideration must be compatible with the material being marked.
 - c. Exempted Markings. Because the classifier’s annotation and origination date are maintained on the drawing specifications, these markings are not required on each piece of classified material. Other markings such as originator identification and unique identification number (accountable material only) do not apply because of the nature of the material.

5. CONTROL SYSTEMS AND ACCOUNTABILITY.

- a. General. Control systems must be established and used to prevent unauthorized access to or removal of classified information. Accountability systems must provide a system of procedures that provide an audit trail. Accountability, as defined below, applies regardless of the physical form of the matter (e.g., electronic, paper, or parts).
- b. Accountable Matter. The following are types of accountable matter:
 - (1) Top Secret matter,
 - (2) Secret matter stored outside an LA (or higher),
 - (3) Any matter that requires accountability because of national, international, or programmatic requirements such as the following:
 - (a) classified computer equipment and media supporting the Nuclear Emergency Support Team (NEST) and Accident Response Group (ARG) operations and similar elements;
 - (b) national requirements such as cryptography and designated COMSEC;
 - (c) international requirements such as North American Treaty Organization (NATO) ATOMAL, designated United Kingdom documents, or other FGI designated in international agreements;
 - (d) designated SAPs; and
 - (e) Sigma 14.
 - (4) Classified Removable Electronic Media (CREM), which is required to be marked as S/RD or higher classification, or which is otherwise accountable (see paragraphs 5.b.(2) and (3) above). Each piece of accountable CREM (ACREM) must remain in accountability until verification that none of the information that requires the CREM to be accountable can be retrieved or recovered from that piece of CREM. Only National Security Agency-approved methods or other officially approved methods that comply with DOE cyber security policy may be used to determine whether information is recoverable from ACREM. Any such approved methods or criteria must be performance-tested as necessary to ensure that unauthorized access to classified information does not occur.
- c. Accountable Classified Removable Electronic Media (ACREM) Custodians.
 - (1) At least one appointed and trained ACREM custodian and alternate ACREM custodian must be assigned for each secure storage repository or

file cabinet used to store ACREM. If more than one custodian and one alternate custodian are assigned, the number of individuals assigned to these positions must be identified and justified through documented cognizant security authority-approved procedures and must be kept to the minimum number necessary based on operational need and associated risk.

- (2) These appointed individuals are responsible and accountable for ACREM, all accountability records, and other duties outlined in cognizant security authority approved local procedures that must include, but are not limited to: a documented ACREM check out and transfer process implemented to record all ACREM transfers between ACREM custodians, alternate ACREM custodians, and users. This process must be performance-tested to ensure its effectiveness.
- d. Control Stations. Control stations must be established to maintain records, accountability systems, access lists (when required), and control classified matter (including facsimiles) received by and/or dispatched from facilities. Control station operators must maintain accountability systems for accountable matter. A defined and operated ACREM accountability process may function as a control station.
 - e. Accountability Records. Accountability records are required when accountable matter is originated, reproduced, transmitted, received, destroyed, permanently buried, or changed in classification. All sites must develop procedures to ensure that all accountable matter has been entered into accountability systems. At a minimum, accountability records must indicate the following information for each item of accountable matter. If accountable matter is received from another agency and lacks a unique identification number, one must be assigned.
 - (1) Date of the Matter. The date the matter was originated or created. For documents, this term means the date the document was finalized.
 - (2) Brief Description of the Matter (unclassified, if possible). Examples include the unclassified title (if a document) or description (if material). It may also be helpful to describe the form of the matter (e.g., a document, magnetic medium, microform, drawing, photograph, or photographic negative). If a title or description is classified, an unclassified descriptor should be used to prevent the accountability records system from becoming classified.
 - (3) Unique Identification Number. This could be a unique document number (if a document) or serial number (if material). Unique identification numbers may be provided by creating a totally new number for each individual document, including copies, or by adding the copy and series to the old base number when reproducing accountable documents. The key

point is to ensure that each document, whether an original or a reproduction, has some kind of unique number associated with it.

- (4) Classification Level (and Category, if RD or FRD) and Caveats. Classification level, category (if RD or FRD), and additional handling caveats, if any, of the matter must also be indicated.
- (5) Number of Copies and Disposition. The number of copies of a document (including the original) generated during either origination or reproduction, the disposition of each copy (e.g., destruction, downgrading, declassification, dispatch outside the facility, or incorporation into another accountability record), and the date of disposition. The term “disposition” varies in meaning as follows regarding:
 - (a) origination, transmission, receipt, and reproduction, “disposition” means the offices or activities where the matter was distributed;
 - (b) destruction, “disposition” means the organization where the matter was destroyed and by whom;
 - (c) change of classification, “disposition” means which office or activity performed the change of classification and which offices or activities have copies of the matter.
- (6) Originator Identification. The organization name and address of the originator. For material, this information is found in the associated paperwork.
- (7) Authority for Contractor Retention. Contract or other written retention authority that authorizes the matter to be in the possession of a contractor. This authorization can be either a letter of authorization or a contract reference to the authorization to retain classified matter. A copy of this authorization should be maintained with the accountability records and should be readily available to facilitate compliance disposition reviews.
- (8) Date Received (if applicable). The date the transmitted matter arrived.
- (9) Activity from Which the Matter was Received (if applicable). The office or activity name and address from which matter was transmitted to the recipient.
- (10) Responsible Individual. The individual who checked it in and/or out (who has personal responsibility for it).

f. Accountable Material.

- (1) General. Accountability procedures must be approved by the cognizant security authority.

- (2) Exemptions. When they are *not* applicable, the following items are exempt from inclusion in the material accountability records:
 - (a) matter date;
 - (b) number of copies; and
 - (c) date and disposition of reproduction.
- (3) Requirements. The material accountability system must provide a description of each type of item, the classification level and category (if RD or FRD), the number of items of each type, and scheduled inventories. Part numbers and serial numbers should be used, when available, as a unique number or to identify the types of material. Where applicable, the production cycle and production control procedures can be used to facilitate the conduct of all inventories of accountable material.

g. Inventory.

- (1) Frequency.
 - (a) All ACREM must be inventoried and all results documented on a recurrent basis. All discrepancies between ACREM records and the verified locations and status of all ACREM, must be identified and reconciled (examples of status include possessed by an identified individual, stored, or destroyed).
 - 1 The current and previous individual assigned control/possession of all ACREM, according to their assigned custodians and users, must be documented and available at any given time within record retention periods. Inventories and resolution of discrepancies must be used to validate that local ACREM custodians, alternate custodians, users, and procedures are meeting this performance requirement;
 - 2 The baseline required frequency of the recurrent ACREM inventories is monthly (no longer than 31 calendar days between inventories). However, the DOE cognizant security authority may increase the time between inventories up to a maximum of six months. The DOE cognizant security authority's decision to decrease inventory frequency must be based on a documented determination that doing so will result in no unacceptable increased risk to the ACREM. Factors to consider in making this determination include:

- a the amount of ACREM;
 - b the number of formally appointed ACREM custodians and alternate custodians;
 - c ACREM usage levels;
 - d strength of the local Classified Matter Protection and Control Program;
 - e characteristics of the local facilities, equipment and procedures; and
 - f past performance in managing ACREM.
- 3 Inventories are not required for ACREM maintained in a locked file cabinet or General Services Administration (GSA) approved security container that is located in a vault or a VTR, or is maintained in security containers with XO-Series locks, and the container has not been accessed since the last inventory. However, time between inventories must not exceed 1 year (365 calendar days) for any ACREM.
- (b) National Nuclear Security Administration's (NNSA) Nuclear Emergency Search Team (NEST), Accident Response Team (ARG), and similar elements' classified computer equipment and media (non-ACREM) must be inventoried at least once a month by two individuals. In addition, DOE cognizant security authorities must develop deployment and redeployment checklists for all ARG, NEST, and similar elements that include procedures for inventorying accountable equipment both before and after a deployment.
- (c) All other accountable matter must be inventoried no less frequently than every 12 months.
- (2) Inventories must consist of a physical comparison of each item against the current inventory listing. Discrepancies must be resolved, if possible using the previously reconciled inventory and receipts, transfers and destruction records. Each item listed in an accountability record must be verified visually.
- (3) Reports. Any unresolved discrepancies between the items found to be present and the inventory list must be reported and dealt with according to DOE policy and requirements for reporting incidents of security concern (see DOE M 470.4-1 Chg. 1).

- h. Master Files and Databases. Master files and databases created in central data processing facilities to supplement or replace Top Secret records are *not* authorized for disposal under National Archives and Records Administration's General Records Schedule 18. These files must be scheduled on an SF 115, *Request for Records Disposition Authority*.
 - i. Automated Accountability Systems and Electronic Receipting.
 - (1) Automated Accountability Systems. Automated accountability systems must:
 - (a) be approved by the DOE cognizant security authority;
 - (b) implement the requirements under paragraph 5.e. above; and
 - (c) provide security controls to ensure that no unauthorized changes are made to system records.
 - (2) Electronic Receipting. Electronic receipting systems are approved as long as the following conditions are met. The system:
 - (a) is approved by the DOE cognizant security authority;
 - (b) provides identification of both the individual and the document disposition; and
 - (c) provides adequate security controls to ensure that no unauthorized changes are made to the system record.
6. REPRODUCTION.
- a. General.
 - (1) Cognizant security authority-approved procedures must be established for the reproduction of classified matter. Reproduction of classified matter must be limited to the minimum number of copies consistent with operational requirements and any other pertinent reproduction limitations. Local procedures should address the issue of controlling the number of copies of classified documents.
 - (2) Reproduction must be accomplished by authorized persons who know the procedures for classified reproduction and only in the performance of official or contractual duties.
 - (3) Classified documents may be reproduced without originator approval except when they contain markings that limit reproduction.

- (4) To restrict reproduction of a classified document, consider one of the following techniques.
 - (a) For intelligence documents only, the Originator Controlled (ORCON) caveat marking may be used to restrict reproduction to that allowed by the originator.
 - (b) Originators of non-intelligence documents who wish to prevent unlimited copying of a classified document may use the markings restricting duplication without originator approval.
 - (5) When any of the data that reside on a piece of ACREM (source media, in this case) is moved to, or reproduced on, another piece of media, the receiving media immediately becomes (or remains) accountable because it must be assumed to contain that which made the source media accountable, until proven otherwise and approved by the DOE CSA.
- b. Equipment. Classified matter must be reproduced on equipment specifically approved and designated for this purpose to ensure minimal risk of unauthorized disclosure or access. To the greatest extent possible, this equipment must be located within LAs, PAs, EAs, or MAAs.
- (1) Access to Machines. Classified copying must not be performed in the presence of individuals lacking the proper security clearances or need to know.
 - (2) Approval. Ensure all machines to be used for reproducing classified documents are approved in accordance with local procedures and cyber security policy.
- c. Documents Received From Outside Agencies. Outside agency documents may be reproduced in accordance with the same rules and restrictions that exist for DOE documents. Therefore, unless specific instructions to the contrary accompany the documents, they may be reproduced. For example, National Security Council (NSC) documents will have a copy restriction notice; therefore, NSC documents will be reproduced only with the permission of the originator.

7. RECEIVING AND TRANSMITTING CLASSIFIED MATTER.

- a. General. Classified matter must be transmitted only in the performance of official or contractual duties. If the transmission is not required by the specific terms of the contract or required for performance of the contract, contractors must obtain written authorization from the DOE cognizant security authority before transmitting classified matter outside the facility. Before transmitting classified matter, the sender must ensure:

- (1) The recipient has the appropriate security clearance, has any required programmatic or special access approval, and meets the need-to-know criteria.
 - (2) An approved classified address has been identified and used for the appropriate method of transmission, e.g., mailing, shipping, or overnight delivery.
- b. Receiving. When classified matter is received at a facility, the following controls must apply (also see paragraph 7.d. below):
 - (1) Classified matter must be delivered to personnel designated to receive it at a control station with the inner envelope unopened. Procedures must be established to ensure that when classified matter is not received directly by the designated control station (regardless of the type of mail system), the inner container remains unopened.
 - (2) The package must be examined for evidence of tampering and the classified contents checked against the receipt (if provided). Evidence of tampering must be maintained and reported promptly to the cognizant security authority. If the matter was received through the U.S. Postal Service, the appropriate U.S. Postal Inspector must also be notified promptly. Discrepancies in the contents of a package must be reported immediately to the sender. If the package (or container) is in order and includes a receipt, the receipt must be signed and returned to the sender.
- c. Packaging. Classified matter to be transmitted outside a facility must be double-wrapped (enclosed in opaque inner and outer containers) except as specified below. The contents of the package or shipment must be securely packaged to meet DOE and the applicable transporting agency's requirements, i.e., the U.S. Postal Service, for transmission.
 - (1) Envelopes and Similar Wrappers. All classified information physically transmitted outside facilities must be enclosed in two layers, both of which provide appropriate protection and reasonable evidence of tampering and which conceal the contents. The inner enclosure must clearly identify the classified address of the sender and the intended recipient, the highest overall classification level, and category (if RD or FRD), of the contents, and any appropriate warning notices. The outer enclosure must be the same except that no markings to indicate that the contents are classified must be visible. Intended recipients must be identified by name only as part of an attention line.
 - (2) Other Containers. The outer container must maintain the integrity of the inner container.

- (a) As long as the item is enclosed in a double container, the matter may be wrapped or boxed in paper, wood, metal, or a combination thereof.
- (b) If a locked briefcase is used to hand-carry classified matter of any level, the briefcase may serve as the outer container. A briefcase must not serve as the outer container for travel aboard public transportation.
- (c) The outer container must be addressed to a classified address, return-addressed to a classified mailing address, and sealed, with no markings to indicate the contents are classified.
- (d) If specialized shipping containers, including closed cargo transporters, are used for transmitting classified matter, the shipping container can be considered the outer container.

(3) Equipment Components.

- (a) If the classified matter is an internal component of a packaged item of equipment with an outside shell or body that is unclassified and that completely shields the classified internal component from view, the shell or body may be considered the inner container. If the shell or body is used as the inner container the address and return address may be omitted.
- (b) If the classified matter is an inaccessible internal component of a bulky item of equipment, such as a missile, that cannot be reasonably packaged, no inner container is required and the outside shell or body may be considered the outer container if it is unclassified.

d. Offsite Transmittal and Receipts. When transmitting secret or accountable classified matter outside site/facilities by any method, a receipt must be used. Receipts must identify the classified contents and the names and addresses of both the sending and receiving facilities. Receipts must not contain classified information. If not practical, the receipt may be sent to the recipient with the required advance notification of shipment or may be hand-carried. When classified matter is transmitted by courier, DOE F 5635.3, *Classified Document Receipt*, or a receipt comparable in content must be used.

- (1) Receipt Information. The receipt must be prepared in triplicate and remain unclassified when completed. Two copies of the receipt must be placed in the inner container with the matter (except as noted above) and sent to the intended recipient. The third copy must be maintained by the sender until the original is signed and returned. The receipt must contain the following information:

- (a) full names of the sender and the recipient;
 - (b) unclassified address of the sender, unless the receipt contains classified information and a classified mailing address for the sender is required;
 - (c) classified address of the recipient;
 - (d) description of the classified matter (e.g., title or other means);
 - (e) date of the matter;
 - (f) classification of the matter; and
 - (g) unique identification number, if accountable.
 - (2) Multiple Recipients. A separate receipt must be completed for each recipient regardless of the number of items for each recipient.
 - (3) Facsimile Transmission. Individuals transmitting classified information through facsimile systems must confirm and document receipt with the intended recipient.
 - (4) Returning Receipts. The recipient of any classified matter that contains a receipt must complete the receipt and return it to the sender as soon as possible, but no longer than 30 days following receipt of matter. A copy of the receipt must be maintained with the control station records.
 - (5) Receipt Tracking. Procedures should be established for both tracking the return of receipts and the actions required if receipts are not returned.
 - (6) Electronic Receipting System. Any electronic receipting system must be approved by DOE cognizant security authority. The system must be able to identify the custodian of the classified matter or the disposition, and ensure signature authentication.
- e. Classified Addresses.
- (1) Classified addresses must be verified through the Safeguards and Security Information Management System (SSIMS) or the Defense Security Service (DSS). If not in either system, a new classified mail channel must be established. See DOE M 470.4-1 Chg. 1 for additional requirements.
 - (2) Hard-copy printouts of the SSIMS or DSS classified addresses can only be used to validate approved classified addresses for 30 calendar days from print date.

- f. Transmittal and Receipt within Facilities. Classified matter may be transmitted within a facility without single or double-wrapping provided adequate security measures are taken to protect the matter against unauthorized disclosure.
 - (1) Although double-wrapping is not required for classified matter transmitted within a facility, the transmittal method should dictate the most suitable method of protection.
 - (2) The matter may be transmitted by approved electronic means. When using this method, both the transmitting and receiving systems must be approved for the classification level and category of the information to be transmitted. Facilities also must have an approved security plan and procedures for transmitting the information by electronic means.
- g. Transmitting Confidential Matter Outside of Facilities.
 - (1) Confidential matter must be transmitted by any of the following methods or any method approved for the transmission of Secret or Top Secret matter.
 - (2) U.S. Postal Service Certified Mail is authorized within the 50 States, the District of Columbia, Puerto Rico, and U.S. territories or possessions. A return mail receipt is not required; however, if the parcel does not arrive at the appointed destination, action may be taken to obtain a receipt. A return receipt may be requested before or after delivery for all Certified Mail and Registered Mail. NOTE: OGAs may use First Class Mail; but First Class Mail is not authorized for DOE.
 - (3) DOE and DOE contractors may receive Confidential matter from OGAs through U.S. Postal Service Express Mail. However, the use of the U.S. Postal Service Express Mail is not permitted for the transmission of Confidential matter by DOE and DOE contractors.
- h. Transmitting Secret Matter Outside of Facilities.
 - (1) Secret matter must be transmitted by one of the following ways or by any method approved for the transmission of Top Secret matter.
 - (2) Postal/Mail Services.
 - (a) U.S. Postal Service Registered Mail is authorized within the 50 States, the District of Columbia, and Puerto Rico. A return receipt is not required for U.S. Postal Service Registered Mail.
 - (b) U.S. Registered Mail through Army, Navy, or Air Force Postal Service facilities, provided approval is obtained from the Office of Health, Safety and Security and information does not pass out of U.S. citizen control or through a foreign postal system. This

method may be used to transmit Secret matter to and from U.S. Government or U.S. Government contractor employees or members of the U.S. armed forces in a foreign country. A return mail receipt is not required.

- (c) Canadian registered mail with registered mail receipt to and between the United States Government and Canadian Government installations in the 50 States, the District of Columbia, and Canada.
 - (d) DOE and DOE contractors may receive Secret matter from OGAs through U.S. Postal Service Express Mail. U.S. Postal Service Express Mail is not permitted for the transmission of Secret matter by DOE and DOE contractors.
 - (e) Approved commercial express service organizations in accordance with the provisions contained in paragraph 7.k. below.
 - (f) Approved common carrier services with escorts who possess the appropriate security clearance in accordance with paragraph 7.l. upon approval by the cognizant security authority.
- i. Transmitting Top Secret Matter Outside of Facilities. Top Secret matter must be transmitted in one of the following ways after approval by the DOE cognizant security authority:
 - (1) by the Defense Courier Service,
 - (2) the Department of State Courier System if outside the United States and its territorial areas,
 - (3) over approved communications networks (see DOE O 200.1, *Information Management Program*, dated 9-30-96, for requirements), or
 - (4) by individuals authorized to hand-carry Top Secret matter in accordance with paragraph 7.j. below.
- j. Hand Carrying. The following requirements apply to hand-carrying classified matter; however, the requirements identified in paragraph 7.l. below, also apply to hand-carrying bulk documents.
 - (1) Local procedures must be developed describing the process for obtaining approval (including approval authority) to hand-carry outside of a site/facility and for providing notification when removing classified matter from the facility. Local hand-carry procedures must be approved by the cognizant security authority.
 - (2) A record/receipt of the classified matter must be made before departure, retained by the employee, and inventory must be made of the matter for

which the employee was charged. The record should contain the following information:

- (a) subject or title (unclassified, if possible);
 - (b) date of the matter;
 - (c) date the matter was removed from the facility;
 - (d) signature of the person removing the matter; and
 - (e) date the matter was returned; or date and recipient's name and organization from receipt for matter that was transferred to another individual.
- (3) The removal of classified matter from approved facilities to private residences or other unapproved places (e.g., hotel or motel rooms) is prohibited.
- (4) Contingency plans for delayed arrival must cover alternative protection and storage procedures, reporting requirements, and be approved by the cognizant security authority.
- (5) Classified matter may be hand-carried outside the United States, provided the following conditions are met.
 - (a) The traveler must possess appropriate security clearance and a diplomatic passport. Diplomatic passports can only be issued to Federal personnel attached to a mission or embassy as a tenant or performing a mission under the auspices of the Department of State.
 - (b) The traveler must obtain written authorization from the cognizant Departmental element.
- (6) Requirements for security screening of classified matter at airports are established by the Transportation Security Administration (TSA).
- k. Approved Commercial Express Service Organizations. The use of commercial express service organizations for transmitting classified matter is restricted to emergency situations and the matter must be delivered to and secured at the receiving location the next calendar day.
 - (1) General. At a minimum, the sender must ensure that the following conditions are met.
 - (a) The use of the express service organization has been approved by the sender's DOE CSA and an address for receiving deliveries

from the express service has been input into SSIMS for the receiving organization.

- (b) The address selected for the overnight/commercial express service cannot be greater than five lines, *cannot* be a post office box, and must be a street address.
- (c) The intended recipients must be notified 24 hours in advance (or immediately if transit time is less than 24 hours) of the proposed shipments and arrival dates.
- (d) All packages are double-wrapped before being inserted into the packaging provided by the commercial express service organization.
- (e) In accordance with packaging requirements, commercial express service packages must not be identified as classified packages.
- (f) The properly wrapped packages are hand-carried to the express mail dispatch center or picked up from a control station in sufficient time to allow for dispatch on the same day.
- (g) Commercial express carrier drop boxes must not be used for classified packages.
- (h) Facilities should include specific details regarding the use of package tracking in local procedures. The commercial express carrier may be contacted for details regarding packaging requirements.

- (2) Problems. Problems with the delivery of classified matter via commercial express service delivery must be reported in accordance with reporting of security incidents (see DOE M 470.4-1 Chg. 1).

- I. Common Carrier Services. Common carrier services include all modes and means of transport (e.g., air, rail, vehicular, and intercity messenger services) excluding express service organizations. The following requirements apply to the use of such commercial services as well as for bulk shipments of classified matter.

- (1) General.

- (a) The contents must be securely packaged to meet DOE and Department of Transportation requirements for transmission.
- (b) Seals or other tamper-indicating devices approved by the cognizant security authority must be placed in a manner to show evidence of tampering on all freight and/or bulk shipments other than overnight commercial express packages. Seals must have serial numbers,

which must be entered on bills of lading or other shipping papers. Seal numbers must be verified by the consignee upon arrival of a shipment.

- 1 Whenever practical, combination padlocks meeting Federal Specification FF-P-110, Padlock, Changeable Combination must be used to secure closed cargo areas of vehicles, vans, and railroad cars.
- 2 Shipments of Secret or Confidential matter received at common carrier terminals must be picked up by the consignee on the day of arrival unless the carrier provides continuous protective service to the address of the consignee under locally approved procedures.

(2) Assurances and Notifications.

- (a) Notification of shipments must be transmitted to the consignee before departure with 24-hour advance notice (or immediately upon dispatch if within 24 hours) to enable proper handling at the destination. At a minimum, the notification must include the nature of the shipment, means of shipment, number of seals, anticipated time and date of arrival, and requested notification if not received by a specified time.
- (b) The consignee must advise the consignor of any shipment not received within 24 hours after the estimated time of arrival furnished by the consignor or trans-shipping activities personnel. Upon receipt of such notice, the consignor must immediately begin tracing the shipment.

(3) Protective Measures. Protective measures for Departmental security shipments are as follows.

- (a) Sufficient personnel with appropriate security clearance must be tasked for a specific movement assignment to ensure continuous protection of the matter being transported;
- (b) At a minimum, the common carrier service must be required to provide the following security services;
- (c) surveillance by an authorized carrier employee with appropriate security clearance when the classified matter is outside the vehicle;
- (d) a tracking system that ensures prompt tracing of the shipment while en route;

- (e) an alarmed or guarded storage area with immediate response by a carrier employee, commercial guard, or police officer when storage is required; and
- (f) When shipments are transported by rail or motor vehicle, personnel escorting the shipments must keep the shipment car(s) under observation, maintain continuous vigilance for conditions or situations that might threaten the security of the cargo, and take appropriate actions as circumstances require. During stops or when practical and time permits, personnel escorting shipments must check the cars, container locks, and/or tamper-indicating devices.

8. DESTRUCTION.

- a. Local procedures must be established for the ongoing review of classified holdings (e.g., multiple copies, obsolete matter, classified waste) to reduce volume to the minimum necessary.
- b. If under a court order prohibiting destruction, special destruction procedures may be required. Under such circumstances, all destruction activities must be conducted in accordance with guidance provided by the DOE Office of General Counsel and the appropriate records management organization.
- c. Classified matter must be destroyed beyond recognition to preclude subsequent access to any classified information. Electronic storage media (ESM) must be destroyed in accordance with the DOE cyber security directives. Destruction techniques include burning, shredding, pulping, melting, mutilating, pulverizing, or chemical decomposition. The following additional requirements must be satisfied when classified matter is destroyed.
 - (1) The DOE cognizant security authority must approve the use of public destruction facilities and any other alternative procedures used by contractors.
 - (2) If classified matter cannot be destroyed onsite, it may be destroyed at a public destruction facility. If a public destruction facility is used, an appropriately cleared individual must ensure the destruction occurs on the same day it leaves a cleared facility and that the destruction is properly witnessed. A record of dispatch is required when the matter is released to another cleared contractor or OGA.
 - (3) Ash residue produced by burning must be examined and reduced by physical disturbance to ensure that the matter is completely destroyed and no ash residue matter remains to prevent the release of classified information or subsequent analysis.

- (4) Classified microforms must be destroyed by burning, chemical decomposition, disintegration, or other methods approved by the cognizant security authority.
 - (5) Classified ESM destruction must include examination to ensure that the media is no longer usable and that no classified information is present or recoverable. Classified ESM destruction must be completed in accordance with the DOE cyber security requirements.
- d. Equipment. Classified matter must be destroyed by equipment that has been approved by the cognizant security authority and in accordance with specific manufacturer's instructions. The residue output must be inspected each time destruction is effected to ensure that established requirements have been met.
 - (1) Shredders.
 - (a) Crosscut shredders used for the destruction of classified paper matter and non-paper products, excluding microfilm, must produce residue with a particle size not exceeding 1 mm in width by 5 mm in length. (Note exception in following paragraph.)
 - (b) Crosscut shredders purchased prior to December 31, 2003 that produce residue with a particle sizes not exceeding 1/32 of an inch in width by 1/2 inch in length may continue to be used for the destruction of classified paper matter and non-paper products, excluding microfilm. However, these shredders must not be used once they cannot be repaired or restored to cut residue within the 1/32-inch width by 1/2-inch maximum particle dimensions.
 - (2) Pulping equipment must be equipped with security screens with perforations of 1/4 inch or smaller.
 - (3) Pulverizing equipment must be outfitted with security screens that meet the following specifications:
 - (a) Hammer mill perforations must not exceed 3/16 inch in diameter.
 - (b) Chopper and hybridized disintegrator perforations must not exceed 3/32 inch in diameter.
- e. Witnesses.
 - (1) The destruction of classified matter must be ensured by an individual(s) who has/have appropriate security clearance for the classification level, category (if RD/FRD), and any applicable caveats of the matter to be destroyed.

- (2) The destruction of non-accountable classified matter may be accomplished by one individual; no witness is required.
- (3) The destruction of accountable classified matter must be witnessed by an appropriately cleared individual other than the person destroying the matter.

f. Destruction Records.

- (1) Accountable Matter. Destruction of accountable classified matter must be documented on DOE F 5635.9, *Record of Destruction*, or a form similar in content, which must be signed by both the individual destroying the matter and the witness.
- (2) Non-accountable Matter. Non-accountable matter does not require destruction receipts or certificates.

9. FOREIGN GOVERNMENT INFORMATION. The requirements in this paragraph are provided in addition to other protection and control measures in this CRD and are not applicable to NATO information. NATO information must be safeguarded in compliance with the U.S. Security Authority for NATO Instructions. Modifications to these requirements may be permitted by treaties, agreements, or other obligations with the prior written consent of the national security authority of the originating government.

- a. General. FGI must be safeguarded to provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When equivalent, standards may be less restrictive than the safeguarding standards that ordinarily apply to U.S. Confidential information, including allowing access to individuals with a need to know who have not otherwise been cleared for access to classified information.
- b. Classified Information Received from Foreign Governments. To ensure the protection of classified FGI in accordance with Executive Order 12958, as amended, the following requirements must be met.
 - (1) Handling. Classified documents received from foreign governments do not require portion marking. Such documents generated and marked entirely by a foreign government must be protected commensurate with the classification level the foreign government specified.
 - (2) Marking.
 - (a) A derivative classifier or classification officer must be contacted with any questions regarding the appropriate classification level for a FGI document.
 - (b) Documents generated by a foreign government in which U.S. information has been added must be reviewed for classification by

a derivative classifier or classification officer, marked, and protected accordingly.

- (c) If the original markings in the foreign government documents are readily recognizable as related to a U.S. classification requiring special protection and control, the documents do not require re-marking.
 - (d) If the foreign government marking is not readily recognizable as related to a U.S. classification, the foreign government document must be reviewed by a derivative classifier or classification officer, and an equivalent U.S. classification must be applied.
 - (e) If the fact that the information is FGI must be concealed, the document must be marked as if it were wholly of U.S. origin.
- (3) Confidential Foreign Government Information. Unless requested by the originating government, records are not required to be maintained for Confidential FGI.
 - (4) Secret Foreign Government Information. Secret FGI must be entered into accountability when required by treaties or international agreements.
 - (5) Top Secret Foreign Government Information. Top Secret FGI must comply with the requirements in paragraph 5 above.
 - (6) Confidential Foreign Government Information–Modified Handling Authorized (C/FGI-MOD). If the foreign protection requirements are lower than the protection required for U.S. Confidential information, the following requirements must be met.
 - (a) Marking. If a document is determined to be C/FGI-MOD, in addition to other marking requirements above, the first page of the document must include:
 - 1 the derivative classifier marking, unless C/FGI-MOD can be determined by foreign markings, and
 - 2 the statement, “This document contains (*name of country*) (*classification level*) information to be treated as U.S. Confidential-Modified Handling Authorized.”
 - 3 The DOE F 470.9, *C/FGI-Mod Coversheet*, must be used.
 - (b) Access/Need to Know. Access to C/FGI–MOD matter does not require DOE security clearance. However, such documents must be provided only to those who have an established need to know and where access is required by official duties and who are citizens

from countries that have been authorized by the originating country.

- (c) Protection. C/FGI-MOD matter must be protected in the following manner.
 - 1 Protection in Use. Physical control must be maintained over any matter marked as containing C/FGI-MOD matter to prevent unauthorized access to the information.
 - 2 Protection in Storage. C/FGI-MOD matter must be stored to preclude unauthorized disclosure, at least equivalent to that stipulated by the foreign government.
- (d) Reproduction. Matter marked as containing C/FGI-MOD may be reproduced without permission of the originator to the minimum extent necessary to carry out official duties.
- (e) Destruction. When C/FGI-MOD matter is to be destroyed, it must be sufficiently destroyed to preclude recovery of any of the information it contained and in a manner approved for destruction of classified matter or as approved by the DOE cognizant security authority.
- (f) Transmission. C/FGI-MOD matter must be transmitted by means approved for transmitting classified matter unless this requirement is waived by the originating foreign government.

CHAPTER III. STORAGE REQUIREMENTS FOR CLASSIFIED MATTER

1. **STORAGE REQUIREMENTS.** The following physical security storage requirements apply to classified safeguards and security (S&S) interests.
 - a. **Restrictions on Secure Storage Repositories Used for Classified Matter.** Repositories used to store classified matter must not be used to store or contain other items that may be a substantial target for theft.
 - b. **Secure Storage Repository Requirements.** Security containers used for storing classified matter must conform to General Services Administration (GSA) standards and specifications. All GSA-approved security containers must be maintained within limited or higher security areas unless otherwise noted in this CRD. Vaults and vault-type rooms (VTRs) used for open storage of classified matter must meet the requirements of DOE M 470.4-2. (NOTE: The response times in this section do not apply to SAPs or SCI.)
 - (1) Classified matter that is not under the personal control of an individual with appropriate security clearance and need to know must be stored as described below.
 - (a) If inspections by Protective Force (PF) personnel are used as supplemental control, PF personnel must examine exposed surfaces of the secure storage repositories and steel filing cabinets for evidence of any forced entry to ensure that the security container or door is locked and the Standard Form (SF) 702 completely annotated.
 - (b) Areas and buildings must be protected from adversary access by application of GSA-approved locks and barriers. Requirements for these locks and barriers can be found in DOE M 470.4-2.
 - (2) Confidential matter must be stored in the same manner prescribed for Secret or Top Secret matter, but the supplemental controls are not required.
 - (3) Secret matter must be stored as described below or in any manner authorized for Top Secret matter.
 - (a) In a locked vault or in a locked GSA-approved security container within an LA or higher.
 - (b) In a locked VTR within an LA, Exclusion Area (EA), Protected Area (PA), or Material Access Area (MAA) equipped with intrusion detection system protection. PF personnel must respond within 30 minutes of alarm annunciation.

- (c) When located outside an LA, the locked vault or VTR must be under intrusion detection system protection. PF personnel must respond within 15 minutes of alarm annunciation.
- (d) In locked, steel filing cabinets that do not meet GSA requirements (containers purchased and approved for use before July 15, 1994 may continue to be used until October 1, 2012) and are equipped with three-position, dial-type, changeable combination locks. The cabinet must be in a locked area or building within the minimum of an LA. In addition, one of the following supplemental controls is required.
 - 1 Intrusion detection system protection that provides for response from PF personnel within 30 minutes of alarm annunciation.
 - 2 Inspection every 4 hours by PF or by cleared duty personnel when unattended.
- (4) Top Secret matter must be stored as described below.
 - (a) In a locked, GSA-approved security container with one of the following supplemental controls:
 - 1 under intrusion detection system protection and by PF personnel responding within 15 minutes of alarm annunciation; or
 - 2 inspections by PF personnel no less frequently than every 2 hours.
 - (b) In a locked vault or VTR within an LA, EA, PA, or MAA. The vault or VTR must be equipped with intrusion detection equipment, and PF personnel must respond within 15 minutes of alarm annunciation.
 - (c) In a locked vault or VTR within a property protection area (PPA) or outside of a security area, and it must be under intrusion detection system protection. PF personnel must respond within 5 minutes of alarm annunciation.
- (5) Nuclear weapon configurations, nuclear test and trainer devices, and nuclear-explosive-like assemblies without nuclear material must be stored in a vault or VTR located, at a minimum, within an LA. PF personnel must respond within 15 minutes of alarm annunciation. (The DOE physical security manual provides additional requirements.)

- c. Response Personnel. PF personnel, private security firms, or local law enforcement agency personnel must respond to intrusion detection system alarms as specified and documented in the Site Security Plan (see DOE M 470.4-1 Chg. 1 for additional information regarding S&S plans).
 - d. Alternative Storage Locations. Approved Federal Records Centers may be used to store classified information (see DOE M 470.4-1 Chg. 1).
 - e. Commingling Classified Matter.
 - (1) Classified and unclassified documents may be commingled. For example, Top Secret (TS), Confidential (C), and unclassified documents may be stored in the same file folder. Need-to-know considerations, however, might make it necessary to segregate documents (e.g., to avoid photographing Top Secret documents onto the same reel or microfiche as Secret (S) or Confidential documents). Good business practice suggests marking commingled unclassified documents as “Unclassified” when storing/filing with classified documents.
 - (2) Accountable Classified Removable Electronic Media must be separated from and not commingled with other classified information/media.
2. STORAGE—REPOSITORIES. When not in use, classified matter must be stored and locked in an approved secure storage repository unless otherwise noted in this CRD or DOE M 470.4-2. The following storage requirements apply to secure storage repositories that contain classified matter or other S&S interests.
- a. Security Containers.
 - (1) General. Secure storage repositories must not bear any external classification or other markings that would indicate the level of classified matter authorized to be stored within the container. For identification purposes, each security container must bear a uniquely assigned number on the exterior.
 - (2) Accountable Classified Removable Electronic Media (ACREM).
 - (a) All ACREM must be in a LA or higher security area when stored.
 - (b) Secure storage repositories that are used to store ACREM must be configured to provide limited access to ACREM by only the ACREM custodian(s) or alternate ACREM custodian(s).
 - (c) Keys and equivalent mechanisms allowing access to ACREM must be controlled to ensure only authorized ACREM custodians/alternates have access and the control system must be documented.

- (d) A seal must be affixed each time a security container being used to store ACREM that is located outside a vault or VTR is closed, and this action must be documented according to locally approved procedures to provide positive evidence of opening/tampering or access. Alternatively, if the security container is equipped with a XO-series lock prior to opening the container, the authorized opener must operate the lock to display the number of prior openings. The number indicated should correspond to that noted on the SF 702 from the previous opening. (If the number has advanced by one or more integers, the custodian must be alerted that the container had been opened with no record of such on the SF 702 and a security incident report must be filed if required by DOE M 470.4-1 Chg. 1.)

b. Documentation -- SF 700, Security Container Information.

- (1) SF 700, Part 1 must be completed for each secure storage repository or other location approved for storing classified matter and include the names of all individuals who may be contacted if the container is found open and unattended. A record must be maintained of all individuals who have or may be granted access to the secure storage repository combination.
 - (a) The local implementation plan may dictate whether or not Block 8, *Serial No. of Lock*, must be left blank.
 - (b) SF 700, Part 1 must be affixed to the inside of the door of vaults and VTRs containing the combination lock. For security containers, it must be placed inside the locking drawer.
- (2) SF 700, Part 2a must be used to document the combination of the secure storage repository. It must be marked front and back with the highest level and most restrictive category (if RD or FRD) of information that may be stored within the repository and inserted in the accompanying envelope (part 2).
- (3) SF 700, part 2 (envelope) must be marked front and back with the highest level and most restrictive category (if RD/FRD) of information that may be stored within the secure storage repository. Once completed and sealed, it must be forwarded to central records for storage that prevents access by any individual who does not possess the same security clearance, any required formal access approval, and need to know. If the combination protects information requiring additional access approvals (e.g., Sigma 14, Sigma 15, North American Treaty Organization [NATO], Special Access Program [SAP] information, or Sensitive Compartmented Information [SCI]), the Part 2 must not be sent to central records unless all individuals at that location possess the same security clearance, any required formal access approval, and need to know.

- c. Combinations. Combinations to containers containing ACREM must be limited to the responsible ACREM primary and alternate ACREM custodian(s). When there are multiple shifts, the combination can be provided to the ACREM primary and alternate ACREM custodian(s) for each shift. A designated individual may be provided the combination only when the ACREM primary and all alternate ACREM custodian(s) are not available and access is required.
- (1) Changing Combinations. Combinations must be changed by an appropriately cleared and authorized individual as soon as practical after any of the following situations occur.
 - (a) Initial receipt of a GSA-approved security container or lock.
 - (b) When an individual who knows the combination—
 - 1 is reassigned, transferred, or terminated.
 - 2 has his/her security clearance downgraded to a level lower than the level of classified matter stored.
 - 3 has his/her security clearance administratively terminated or suspended.
 - (c) Maintenance is performed by a locksmith or safe technician.
 - (d) When the ACREM custodian(s) and/or alternate ACREM custodian(s) return after the combination has been provided to the designated individual.
 - (e) Compromise or suspected compromise of secure storage repository.
 - (f) Preparation for turning in a completely empty security container.
 - 1 The combination must be set to factory standard 50-25-50 before the container is turned in.
 - 2 When a security container is transferred from one organization to another, the custodian from the original organization must certify, in writing, that all classified matter has been removed before the transfer takes place.
 - (g) Combinations used to protect NATO material must be changed no less frequently than 12-month intervals.
- (2) Selection of Combination Settings. Combination numbers must be selected at random. Security containers with multiple locking drawers must contain a classified combination on each drawer.

(3) SF 701, Activity Security Check List.

- (a) The SF 701 provides a systematic means of checking end-of-day activities for a particular work area, allowing for employee accountability in the event that irregularities are discovered.
- (b) Use of SF 701 is optional except when local security and/or implementation plans require its use for detailed end-of-day security inspections.

(4) SF 702, Security Container Check Sheet.

- (a) The SF 702 must be used to record security checks each day a container may have been accessed by documenting the times and the initials of the person(s) who have opened, closed, or checked a particular container, room, vault, or VTR holding classified information. A sole custodian of a security container is not required to record each opening and closing of the container throughout the day. In such cases, the appropriate information must be recorded on the SF 702 the first time the container is opened that day. The container may be opened and closed as necessary without further record keeping. At the end of the day, information must be recorded indicating the final closing of the container for that day. When 24-hour operations are involved, another reasonable time period may be established to conduct end of the day/shift system checks.
- (b) The SF 702 must be used for any secure storage repository used to store ACREM, including locked drawers or file cabinets in vaults and VTRs and those that use XO-Series locks.
- (c) The SF 702 must be in a conspicuous location and affixed or in close proximity to each security container and/or the entrance to each vault or VTR.

3. NON-CONFORMING STORAGE. Classified matter must be stored under conditions designed to deter and detect unauthorized access to the matter, to include securing it in approved equipment or facilities whenever it is not under the direct control of an authorized person. Non-conforming storage may only be used for classified matter that cannot be protected by the established standards and requirements due to its size, nature, operational necessity, or other factors. In these exceptional cases, non-conforming storage that deters and detects unauthorized access to the classified matter may be used for storing classified matter.

Non-Conforming Storage must result in protection effectiveness equivalent to that provided to similar level(s) and categories of classified matter by standard configurations.

The methods, protection measures, and procedures must be documented and approved by the DOE cognizant security authority. Documentation must include the following:

- a. Explanation as to why exercising this option is necessary;
- b. Description of classified matter to be stored;
- c. Description of the means by which equivalent security is to be provided;
- d. An analysis demonstrating the equivalence of protection;
- e. A copy of the documentation must be maintained locally;
- f. Copies of the documentation must be forwarded to the cognizant Headquarters Departmental element; and
- g. Updates to this documentation as conditions change.

4. PERMANENT BURIAL.

- a. Contractors must submit a request for permanent placement by burial to the DOE cognizant security authority through line management for approval prior to use. In addition to meeting the requirements for non-conforming storage of classified matter, permanent burial request documentation must also include:
 - (1) For active burial operations, description of the entire placement process, including protection of classified matter prior to final burial;
 - (2) Configuration of classified matter to be buried;
 - (3) Assurance that undisturbed burial is designed and will be sustained indefinitely for the buried classified matter;
 - (4) Explanation of current and future use of the burial location and all pertinent location characteristics (natural or engineered) that will limit or preclude access to the classified matter; and
 - (5) Updates to this documentation as conditions change.
- b. Classified matter that is accountable is considered to meet accountability requirements when it is permanently placed into an approved burial configuration.
- c. Inventory of previously accountable classified matter may be suspended indefinitely as long as there has been no access to the matter since it was buried.

SECTION B - OPERATIONS SECURITY

1. OBJECTIVES.

- a. To help ensure that Critical Program Information (CPI) is protected from inadvertent and unauthorized disclosure.
- b. To provide management with the information required for sound risk management decisions concerning the protection of sensitive information.
- c. To ensure that Operations Security (OPSEC) techniques and measures are used throughout the Department.

2. REQUIREMENTS.

- a. An OPSEC program(s) must be implemented covering each site and facility to ensure the protection of CPI and to assist in ensuring the protection of classified matter. The OPSEC program, in addition to ensuring the compliance with the requirements of this CRD, must also include the following activities:
 - (1) Establish a point of contact with overall OPSEC responsibilities for each site and facility whose name and contact information will be provided to the Office of Health, Safety and Security.
 - (2) Ensure OPSEC point of contact participation in the development of local implementation training and/or briefings tailored to the job duties of the individual employees.
 - (3) Development and execution of a comprehensive OPSEC awareness program that includes regular briefings to ensure that personnel are aware of their responsibilities in support of the OPSEC program. These briefings provide local implementation of requirements and may be integrated into, or provided in conjunction with, required security briefings (e.g., new hires' initial briefings, comprehensive or annual refresher briefings).
 - (4) Participation in self-assessments to ensure the requirements to protect and control classified matter and CPI are being followed in all areas and that employees are aware of their responsibilities.
 - (5) Provision of information concerning deviations (e.g., variances, waivers, and exemptions) involving the OPSEC program to the Office of Health, Safety and Security and to the Associate Administrator for Defense Nuclear Security when involving National Nuclear Security Administration (NNSA) facilities, in a timely fashion, to include implementation and expiration of such actions. This may be accomplished through the Field or Site Office Manager as appropriate.
 - (6) Promulgation of new OPSEC requirements to all affected employees.

- (7) Interaction and coordination with Office of Health, Safety and Security on OPSEC National and Departmental requirements interpretation and local implementation activities. Interaction and coordination between NNSA facilities and the Office of Health, Safety and Security is through the Associate Administrator for Defense Nuclear Security.
- b. OPSEC plans must be developed for programs and operations and approved by the cognizant security authority.
- c. OPSEC plans must be reviewed and updated annually (at least every 12 months).
- d. CPI, formerly known as critical sensitive information, must be identified, including operational and programmatic data that would have a negative impact on national security and/or Departmental operations if unauthorized disclosure should occur. The CPI must be:
 - (1) prioritized according to the level of impact posed by an unauthorized disclosure. The CPI may be supported by a list of indicators that, when aggregated and analyzed, inappropriately reveal elements of the CPI.
 - (2) reviewed on a continuing basis. Results of the CPI reviews must be documented and maintained in program files.
- e. OPSEC assessments must be conducted at facilities having Category I special nuclear material (SNM) (or credible roll-up of Category II to a Category I quantity), Top Secret or Special Access Program (SAP) information within their boundaries. OPSEC assessments must be conducted at other facilities involved in creating, handling, storing, processing, transmitting, or destroying CPI as deemed necessary by the cognizant security authority.
 - (1) Either the programmatic or facility approach may be used to conduct OPSEC assessments. If the facility approach is used, all activities at the facility must be included in the assessment. If the programmatic approach is used, all activities within the program must be included in the assessment.
 - (2) When using the programmatic approach, the assessment team must ensure that CPI pertaining to Category I SNM (or credible roll-up of Category II to a Category I quantity), Top Secret matter, or SAPs are assessed. Schedule and priority for conducting assessments will be based on CPI, threat assessments, risk management principles, recommendations received from the local OPSEC program, and direction from Department of Energy (DOE) line management.
- f. OPSEC reviews must be conducted to identify changing priorities in the local OPSEC program. OPSEC reviews are limited information-gathering activities to

provide the data necessary to schedule and implement OPSEC actions. Results of OPSEC reviews must be documented.

- (1) OPSEC reviews of sensitive activities and facilities must be conducted whenever the following criteria are met:
- (2) New construction is planned for a facility that will process or store classified or sensitive information or matter.
- (3) New sensitive activities are initiated or existing programs incur significant changes.
- (4) A sensitive program or activity has not been the subject of an OPSEC assessment or OPSEC review for the preceding 2 years.

g. Information to be posted to publicly available websites.

- (1) Before any information generated by or for the Federal Government (Government Information) is placed on a DOE, DOE contractor or sub-contractor website or is otherwise made available to the public, it must be reviewed to ensure that it does not contain classified information or CPI. Before DOE contractors or sub-contractors post Government Information to a personal or non-DOE website, it must also be reviewed for the same concerns. The review process must include a multi-layer review to ensure suitability of the information for worldwide public release.
- (2) Automated analysis tools should be used to assist in the review of information to determine if it is appropriate to release it to the public. Certain categories of unclassified information are generally recognized as unsuitable for public release. These include, but are not limited to, Official Use Only information, privacy information, protected Cooperative Research and Development Agreement information, Unclassified Controlled Nuclear Information, and Export Control Sensitive Subjects information. Due to the diversity of information that must be considered within DOE, a robust review and approval process must be conducted using the following evaluation factors for determining suitability for release of information to the public. Evaluation factors include:
 - (a) Sensitivity. If the information is released to the public, it must not reveal or identify sensitive information, activities or programs.
 - (b) Risk. Information that may be used by adversaries to the detriment of employees, the public, the Department or the nation must not be approved for release. This determination must be based on sound risk management principles focused on preventing potential adverse consequences.

- (3) Local procedures must be established for conducting information reviews and acquiring approval according to direction from the Head of their respective Departmental element. These procedures must identify specific information and information categories considered unsuitable for release to the public.

SECTION C - SPECIAL ACCESS PROGRAMS

1. OBJECTIVES. To establish requirements for Special Access Programs (SAPs) authorized for use within the Department. (NOTE: Terms and activities such as Limited Access, Controlled Access, and Limited Distribution programs are not authorized.)
2. REQUIREMENTS.
 - a. All SAPs must be approved by the Secretary or Deputy Secretary, based upon the recommendation of the SAP Oversight Committee (SAPOC), which manages and oversees the development of SAP security policies and procedures outlined in DOE M 471.2-3B, *Special Access Program Policies, Responsibilities and Procedures*.
 - b. SAPs must be limited to acquisition, operations, support, and intelligence activities.
 - c. U.S. Department of Energy (DOE) and non-DOE (Work for Others) SAPs, with the exception of intelligence SAPs, must be registered manually (not in the Safeguards and Security Information Management System) through the established Facility Clearance process using DOE F 470.2, Facility Data Approval Record (FDAR) and DOE F 470.1, Contract Security Classification Specification, Department of Defense Form 254, or form similar in content. For additional information regarding the FDAR process, see DOE M 470.4-1 Chg. 1, *Safeguards and Security Program Planning and Management*. The FDAR and other forms must be classified in accordance with classification guidance. SAPs must be manually registered through the SAP Security Coordinator with the DOE SAP Security Program Manager. Intelligence SAPs must be manually registered with the Office of Intelligence and Counterintelligence (IN) in accordance with instructions provided by IN. Registration of all Intelligence SAPs, other than those housed in a sensitive compartmented information facility, will be coordinated between the DOE SAP Security Program Manager and the Intelligence Work for Others Coordinator.
 - d. SAP facilities, work areas and all activities must be surveyed according to DOE M 470.4-1 Chg. 1, *Safeguards and Security Program Planning and Management*, by the cognizant SAP Security Coordinator in coordination with the cognizant program office and/or sponsor. Intelligence SAPs must be surveyed by the Office of Intelligence and Counterintelligence in conjunction with the Sponsor. Independent oversight inspections must be performed for Departmental programs in accordance with DOE M 471.2-3B.
 - e. Protection program planning documents, including security plans and standard operating procedures, must comply with established SAP policies and program security manuals.

- f. Any possible or probable loss, compromise, or unauthorized disclosure of SAP information must be reported to the appropriate Government Program Manager, Government Program Security Officer, DOE SAP Security Program Manager (or Cognizant SAP Security Coordinator) and the SAPOC's Executive Secretary in accordance with established procedures. (DOE M 470.4-1 Chg. 1, *Safeguards and Security Program Planning and Management*, Section N, contains additional requirements.)

SECTION D - TECHNICAL SURVEILLANCE COUNTERMEASURES

This Section is Official Use Only

Please contact the DOE Office of Health, Safety and Security
at (301) 903-0292 to request a copy